Universidad Nacional José Faustino Sánchez Carrión

Facultad de Ingeniería Industrial, Sistemas e Informática

Escuela Profesional de Ingeniería Informática

Sistema de gestión de seguridad de la información y su influencia con la calidad de servicio de las redes LAN en la Municipalidad Distrital de Végueta, Huaura – 2025

Tesis

Para optar el Título Profesional de Ingeniero Informático

Autora

Briguit Natali Ramirez Mendoza

Asesor

Ing. Julio Cesar Barrenechea Alvarado

Huacho – Perú

2026

Reconocimiento - No Comercial – Sin Derivadas - Sin restricciones adicionales

https://creativecommons.org/licenses/by-nc-nd/4.0/

Reconocimiento: Debe otorgar el crédito correspondiente, proporcionar un enlace a la licencia e indicar si se realizaron cambios. Puede hacerlo de cualquier manera razonable, pero no de ninguna manera que sugiera que el licenciante lo respalda a usted o su uso. **No Comercial:** No puede utilizar el material con fines comerciales. **Sin Derivadas:** Si remezcla, transforma o construye sobre el material, no puede distribuir el material modificado. **Sin restricciones adicionales:** No puede aplicar términos legales o medidas tecnológicas que restrinjan legalmente a otros de hacer cualquier cosa que permita la licencia.

UNIVERSIDAD NACIONAL
JOSÉ FAUSTINO SÁNCHEZ CARRIÓN

LICENCIADA

(Resolución de Consejo Directivo N° 012-2020-SUNEDU/CD de fecha 27/01/2020)

Facultad de Industrial, Sistemas e Informática

Escuela Profesional de Ingeniería Informática

INFORMACION DE METADATOS

DATOS DEL AUTOR (ES):		
APELLIDOS Y NOMBRES:	**DNI**	**FECHA DE SUSTENTACIÓN**
Ramirez Mendoza, Briguit Natali	**70752495**	**27 de Abril del 2026**
DATOS DEL ASESOR:		
Apellidos y Nombres:	**DNI**	**CÓDIGO ORCID**
Ing. Barrenechea Alvarado, Julio Cesar	**31923723**	**https://orcid.org/0000-0002-4865-3073**
DATOS DE LOS MIEMROS DE JURADOS – PREGRADO:		
APELLIDOS Y NOMBRES:	**DNI**	**CÓDIGO ORCID**
Ing. Bernal Valladares, Carlos Enrique	**15614554**	**https://orcid.org/0000-0002-7421-9537**
Ing. Quispe Soto, Eddy Iván	**15760232**	**https://orcid.org/0000-0001-9050-0938**
Ing. Gallardo Andrés, Jhonar Angel	**42563646**	**https://orcid.org/0000-0002-9513-3126**

Briguit Natali Ramirez Mendoza

Sistema de gestión de seguridad de la información y su influencia con la calidad de servicio de las redes LAN en la Mu...

UNIDAD DE INVESTIGACIÓN FIISI - PREGRADO 2026

Unidad de Investigación de la FIISI - 2026

Facultad de Ingeniería Industrial, Sistemas e Informática

Detalles del documento

Identificador de la entrega
trn:oid:::1:3502281407

Fecha de entrega
9 mar 2026, 11:41 a.m. GMT-5

Fecha de descarga
9 mar 2026, 11:45 a.m. GMT-5

Nombre del archivo
Borrador_de_Tesis_-_parafraseada_Ramirez_Mendoza.pdf

Tamaño del archivo
2.0 MB

108 páginas

27.302 palabras

151.681 caracteres

20% Similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para ca...

Filtrado desde el informe

- Bibliografía
- Coincidencias menores (menos de 10 palabras)

Exclusiones

- N.º de coincidencias excluidas

Fuentes principales

19% Fuentes de Internet
6% Publicaciones
12% Trabajos entregados (trabajos del estudiante)

Marcas de integridad

N.º de alertas de integridad para revisión

No se han detectado manipulaciones de texto sospechosas.

Los algoritmos de nuestro sistema analizan un documento en profundidad para buscar inconsistencias que permitirían distinguirlo de una entrega normal. Si advertimos algo extraño, lo marcamos como una alerta para que pueda revisarlo.

Una marca de alerta no es necesariamente un indicador de problemas. Sin embargo, recomendamos que preste atención y la revise.

Sistema de gestión de seguridad de la información y su influencia con la calidad de servicio de las redes LAN en la Municipalidad Distrital de Végueta, Huaura – 2025

DEDICATORIA

Dedico este trabajo de investigación a mis padres, por su amor incondicional, esfuerzo y constante apoyo, que han sido el pilar fundamental de mi formación personal y académica. A ellos, por motivarme siempre a seguir adelante y no rendirme ante las dificultades. Extiendo esta dedicatoria a mi familia, por su comprensión, cariño y aliento permanente, que me brindaron la fuerza necesaria para alcanzar esta meta tan importante en mi vida.

AGRADECIMIENTO

Agradezco profundamente a Dios por haberme otorgado la fortaleza, la sabiduría y la perseverancia necesarias para culminar con éxito este trabajo de investigación. A mis padres y familiares, por su apoyo incondicional, confianza y motivación constante a lo largo de este camino. A mis docentes, por su guía, compromiso y dedicación durante mi proceso de formación profesional. Finalmente, a la Municipalidad Distrital de Végueta, Huaura, y a todas las personas que de alguna manera contribuyeron al desarrollo y culminación de este logro académico.

ÍNDICE

DEDICATORIA ..... **vi**
AGRADECIMIENTO ..... **vii**
ÍNDICE DE TABLA ..... **x**
ÍNDICE DE FIGURA ..... **xi**
RESUMEN ..... **xii**
ABSTRACT ..... **xiii**
INTRODUCCIÓN ..... **xiv**
CAPÍTULO I. PLANTEAMIENTO DEL PROBLEMA **15**
1.1. Descripción de la realidad problemática **15**
1.2. Formulación del problema **16**
1.2.1. Problema general 16
1.2.2. Problemas específicos 17
1.1. Objetivos de la investigación **17**
1.1.1. Objetivo general 17
1.1.2. Objetivos específicos 17
1.2. Justificación de la investigación **17**
1.3. Delimitaciones del estudio **19**
CAPÍTULO II. MARCO TEÓRICO **20**
2.1. Antecedentes de la investigación **20**
2.1.1. Antecedentes internacionales 20
2.1.2. Antecedentes nacionales 22
2.2. Bases teóricas **25**
2.3. Bases filosóficas **52**
2.4. Definición de términos básicos **53**
2.5. Hipótesis de investigación **55**
2.5.1. Hipótesis general 55
2.5.2. Hipótesis específicas 55
2.6. Operacionalización de las variables **55**
CAPÍTULO III. METODOLOGÍA **57**
3.1. Diseño metodológico **57**
3.2. Población y muestra **58**

3.2.1. Población 58
3.2.2. Muestra 58
3.3. Técnicas de recolección de datos **59**
3.4. Técnicas para el procedimiento de la información **59**
CAPÍTULO IV. RESULTADOS 62
4.1. Análisis de resultados **62**
4.2. Contrastación de hipótesis **72**
CAPÍTULO V. DISCUSIÓN 78
5.1. Discusión de resultados **78**
CAPÍTULO VI. CONCLUSIONES Y RECOMENDACIONES 80
6.1. Conclusiones **80**
6.2. Recomendaciones **81**
CAPÍTULO VII. REFERENCIAS BIBLIOGRAFICAS 82
7.1. Fuentes documentales **82**
ANEXOS 86

ÍNDICE DE TABLA

Tabla 1. *Sistema de gestión de seguridad de la información* 62
Tabla 2. *Seguridad confidencial* 63
Tabla 3. *Seguridad integral* 64
Tabla 4. *Disponibilidad operativa* 65
Tabla 5. *Cumplimiento normativo* 66
Tabla 6. *La calidad de servicio de las redes LAN* 67
Tabla 7. *Velocidad de transmisión* 68
Tabla 8. *Estabilidad de conexión* 69
Tabla 9. *Disponibilidad del servicio* 70
Tabla 10. *Seguridad de red* 71
Tabla 11. *Prueba de normalidad de las variables sistema de gestión de seguridad de la información y la calidad de servicio de las redes LAN* 72
Tabla 12. *El sistema de gestión de seguridad de la información y la calidad de servicio de las redes LAN* 73
Tabla 13. *La seguridad confidencial y la calidad de servicio de las redes LAN* 74
Tabla 14. *La seguridad integral y la calidad de servicio de las redes LAN* 75
Tabla 15. *La disponibilidad operativa y la calidad de servicio de las redes LAN* 76
Tabla 16. *El cumplimiento normativo y la calidad de servicio de las redes LAN* 77

ÍNDICE DE FIGURA

Figura 1. Ciclo Deming o PDCA 27
Figura 2. Sistema de gestión de seguridad de la información 62
Figura 3. Seguridad confidencial 63
Figura 4. Seguridad integral 64
Figura 5. Disponibilidad operativa 65
Figura 6. Cumplimiento normativo 66
Figura 7. La calidad de servicio de las redes LAN 67
Figura 8. Velocidad de transmisión 68
Figura 9. Estabilidad de conexión 69
Figura 10. Disponibilidad del servicio 70
Figura 11. Seguridad de red 71

RESUMEN

El presente trabajo de investigación estudia: Sistema de gestión de seguridad de la información y su influencia con la calidad de servicio de las redes LAN en la Municipalidad Distrital de Végueta, Huaura – 2025. Esta investigación tiene como objetivo: Conocer el sistema de gestión de seguridad de la información y su influencia con la calidad de servicio de las redes LAN en la Municipalidad Distrital de Végueta, Huaura – 2025. Metodología: El método científico de tipo de investigación utilizado fue clásico, denominado puro o fundamental, el nivel de investigación fue descriptivo - correlacional. Hipótesis: El sistema de gestión de seguridad de la información influye significativamente con la calidad de servicio de las redes LAN en la Municipalidad Distrital de Végueta, Huaura – 2025. Muestra: Estuvo constituido por 52 trabajadores de la Municipalidad Distrital de Végueta, Huaura. Las técnicas de recolección de datos utilizadas en este trabajo fue la encuesta. Los instrumentos que se aplicaron fue cuestionario de preguntas. Finalmente, para la estadística se utilizó el paquete estadístico SPSS 25.0 para la investigación y se tiene en cuenta la interpretación de datos, tablas y figuras estadísticas una vez que se tiene un resultado de conexiones de Spearman que arroja un valor de 0. 736 en la hipótesis general, lo cual es una correlación positiva alta, y finalmente se llega a la conclusión general: El sistema de gestión de seguridad de la información influye significativamente con la calidad de servicio de las redes LAN en la Municipalidad Distrital de Végueta, Huaura – 2025.

Palabras clave: Seguridad confidencial, seguridad integral, disponibilidad operativa, cumplimiento normativo, velocidad de transmisión, estabilidad de conexión, disponibilidad del servicio, seguridad de red.

ABSTRACT

This research study examines the Information Security Management System and its influence on the quality of service of LAN networks in the District Municipality of Végueta, Huaura – 2025. The objective of this research is to understand the Information Security Management System and its influence on the quality of service of LAN networks in the District Municipality of Végueta, Huaura – 2025. Methodology: The scientific method used was classical, also known as pure or fundamental research, and the level of investigation was descriptive-correlational. Hypothesis: The Information Security Management System significantly influences the quality of service of LAN networks in the District Municipality of Végueta, Huaura – 2025. Sample: The sample consisted of 52 employees of the District Municipality of Végueta, Huaura. The data collection technique used in this study was a survey. The instruments used were questionnaires. Finally, the SPSS 25.0 statistical package was used for the research, and the interpretation of data, tables, and statistical figures was considered once a Spearman's rank correlation coefficient of 0.736 was obtained for the general hypothesis, which is a high positive correlation. The general conclusion is that the information security management system significantly influences the quality of service of the LAN networks in the District Municipality of Végueta, Huaura – 2025.

Keywords: Confidential security, comprehensive security, operational availability, regulatory compliance, transmission speed, connection stability, service availability, network security.

INTRODUCCIÓN

El presente trabajo de investigación estudió Sistema de gestión de seguridad de la información y su influencia con la calidad de servicio de las redes LAN en la Municipalidad Distrital de Végueta, Huaura – 2025. De esta manera, La información es altamente reveladora porque depende de factores internos y externos; los autores concluyeron que la información es considerada como uno de los activos más relevantes e importante, y se le debe dar especial cuidado y protección, pues sin ella sería explotada por los ciberdelincuentes a nivel mundial afectando a todo tipo de sectores públicos y privado (Diaz, 2021). Por otro lado, Según Berry, et al. (1989) detalla que "calidad de servicio es la conformidad de los usuarios receptores y realidad en la percepción, lo que los usuarios deseen es la preservación de la información mediante las dimensiones tangibilidad, confiabilidad, tiempo de respuesta, seguridad y empatía". Para ello se ha estructurado la presente investigación en los siguientes capítulos:

En el capítulo I comprende el planteamiento del problema, que es la descripción de la realidad problemática, la formulación del problema, los objetivos de la investigación, la justificación, delimitación de estudio y viabilidad. En el capítulo II el Marco teórico, que comprende los antecedentes del estudio, las bases teóricas y filosóficas que viene ser el tratado especial de las teorías de cada una de las variables estudiadas, definiciones de términos básicos, las hipótesis de investigación y la operacionalización de las variables. En el capítulo III la metodología de la investigación que tiene en cuenta el tipo y diseño de la investigación, población y muestra, técnicas de recolección de datos y las técnicas para el procesamiento de la investigación. En el capítulo IV los resultados de la investigación sus respectivas tablas y figuras que corresponde. En el capítulo V, se tiene en cuenta la discusión de los resultados. En el VI capítulo, las conclusiones y recomendaciones que es el producto final de la investigación, las recomendaciones, las referencias bibliográficas y sus anexos que demuestran evidencias de la investigación.

CAPÍTULO I. PLANTEAMIENTO DEL PROBLEMA

1.1. Descripción de la realidad problemática

Actualmente, las instituciones públicas requieren redes informáticas eficientes, seguras y disponibles para garantizar una adecuada atención al ciudadano y una gestión transparente de los servicios. En este marco, el sistema de gestión de seguridad de la información (SGSI) se convierte en un pilar fundamental para asegurar la confidencialidad, integridad y disponibilidad de los datos y los servicios digitales. No obstante, en diversas municipalidades, este aspecto no ha sido considerado con la importancia que merece, generando brechas tecnológicas que afectan directamente la calidad del servicio ofrecido a través de sus redes LAN.

El estudio se desarrollará en la Municipalidad Distrital de Végueta, provincia de Huaura, durante el año 2025, en un contexto donde la digitalización de los servicios municipales se ha incrementado notablemente debido a los procesos de modernización del Estado. Sin embargo, a pesar de la incorporación de sistemas tecnológicos, se evidencian deficiencias significativas en la calidad de servicio de la red LAN, reflejadas en lentitud, caídas constantes, falta de disponibilidad y problemas de seguridad. Estos aspectos comprometen el acceso de los ciudadanos a trámites virtuales, limitan la eficiencia del personal y generan riesgos frente a posibles ciberataques.

Uno de los problemas más relevantes es la falta de un sistema integral de gestión de seguridad de la información. Se han detectado prácticas inadecuadas en el almacenamiento y transmisión de datos, ausencia de políticas claras de acceso y control de usuarios, así como deficiencias en la respuesta ante incidentes de seguridad informática. Estas condiciones no solo generan vulnerabilidades, sino que también afectan directamente la percepción de calidad y fiabilidad de los servicios brindados por la red LAN institucional.

A pesar de estos problemas, no existen estudios previos en el ámbito local que analicen cómo la implementación de un SGSI podría influir directamente en la calidad del servicio de las redes LAN en gobiernos locales como el de Végueta. Sin una base

técnica y científica, las decisiones en materia de tecnología y seguridad se toman de manera empírica o desorganizada, lo que prolonga las deficiencias actuales.

Este vacío ha sido explorado en otras investigaciones. Por ejemplo, en un estudio de la Universidad Nacional Mayor de San Marcos (2023), se evidenció que las organizaciones que implementaron un SGSI conforme a la norma ISO/IEC 27001 presentaron una mejora del 35 % en la eficiencia de sus redes LAN. Asimismo, un análisis desarrollado en la Universidad Tecnológica del Perú (2022) demostró que la integración de políticas de seguridad redujo significativamente los errores de conexión y mejoró la satisfacción del usuario. Finalmente, en la Municipalidad de Santa María (2024), la aplicación de medidas estructuradas de ciberseguridad logró disminuir las interrupciones del servicio en un 40 %, además de fortalecer la confianza en la gestión pública.

En este sentido, se hace necesario desarrollar una investigación que permita determinar cómo influye el sistema de gestión de seguridad de la información en la calidad de servicio de las redes LAN de la Municipalidad Distrital de Végueta. Esta investigación no solo será útil para mejorar el entorno tecnológico de dicha municipalidad, sino que también puede servir como modelo para otras entidades públicas que enfrentan problemáticas similares. La integración de un SGSI adecuado puede representar una solución integral para garantizar un servicio de red LAN más estable, veloz, seguro y disponible para todos los usuarios internos y externos.

Por tanto, surge la siguiente interrogante: ¿Cómo el sistema de gestión de seguridad de la información influye con la calidad de servicio de las redes LAN en la Municipalidad Distrital de Végueta, Huaura – 2025?.

1.2. Formulación del problema

1.2.1. Problema general

¿Cómo el sistema de gestión de seguridad de la información influye con la calidad de servicio de las redes LAN en la Municipalidad Distrital de Végueta, Huaura – 2025?

1.2.2. Problemas específicos

1. ¿Cómo la seguridad confidencial influye con la calidad de servicio de las redes LAN en la Municipalidad Distrital de Végueta, Huaura – 2025?
2. ¿Cómo la seguridad integral influye con la calidad de servicio de las redes LAN en la Municipalidad Distrital de Végueta, Huaura – 2025?
3. ¿Cómo la disponibilidad operativa influye con la calidad de servicio de las redes LAN en la Municipalidad Distrital de Végueta, Huaura – 2025?
4. ¿Cómo el cumplimiento normativo influye con la calidad de servicio de las redes LAN en la Municipalidad Distrital de Végueta, Huaura – 2025?

1.1. Objetivos de la investigación

1.1.1. Objetivo general

Conocer el sistema de gestión de seguridad de la información y su influencia con la calidad de servicio de las redes LAN en la Municipalidad Distrital de Végueta, Huaura – 2025.

1.1.2. Objetivos específicos

1. Conocer la seguridad confidencial y su influencia con la calidad de servicio de las redes LAN en la Municipalidad Distrital de Végueta, Huaura – 2025.
2. Conocer la seguridad integral y su influencia con la calidad de servicio de las redes LAN en la Municipalidad Distrital de Végueta, Huaura – 2025.
3. Conocer la disponibilidad operativa y su influencia con la calidad de servicio de las redes LAN en la Municipalidad Distrital de Végueta, Huaura – 2025.
4. Conocer el cumplimiento normativo y su influencia con la calidad de servicio de las redes LAN en la Municipalidad Distrital de Végueta, Huaura – 2025.

1.2. Justificación de la investigación

a) Justificación ambiental

La implementación de un sistema de gestión de seguridad de la información en la Municipalidad Distrital de Végueta puede aportar significativamente a la sostenibilidad ambiental mediante el uso eficiente de tecnologías que reducen el

consumo innecesario de recursos físicos. Al promover una mayor digitalización y protección de la información, se reduce el uso de papel y otros insumos, fomentando prácticas más responsables con el entorno. Asimismo, un entorno digital seguro y bien gestionado facilita el control de proyectos ambientales, permitiendo un mejor seguimiento de los impactos ecológicos y asegurando que los datos relevantes se almacenen y utilicen de forma responsable. De esta manera, se impulsa una gestión municipal más alineada con los principios de sostenibilidad y protección del medio ambiente.

b) Justificación social

Desde un enfoque social, la implementación de un sistema de gestión de seguridad de la información en la Municipalidad de Végueta contribuye a fortalecer la confianza ciudadana en los servicios públicos digitales. Una red LAN segura y de calidad asegura el acceso confiable a la información y garantiza la confidencialidad y disponibilidad de los datos de la población. Esto favorece la transparencia institucional, promueve una mayor participación ciudadana y mejora la percepción de la eficiencia administrativa. Además, al contar con servicios tecnológicos estables y protegidos, se refuerzan los vínculos entre la institución y la comunidad, creando un entorno más seguro, inclusivo y moderno, orientado al bienestar de todos los ciudadanos.

c) Justificación económica

En el ámbito económico, un sistema de gestión de seguridad de la información eficaz permite optimizar los recursos tecnológicos y reducir los costos operativos derivados de pérdidas de datos, ataques informáticos o interrupciones de red en la Municipalidad Distrital de Végueta. Al asegurar la integridad y disponibilidad de la información, se mejora la toma de decisiones basada en datos confiables, lo que permite una mejor planificación y ejecución presupuestal. Además, una red LAN eficiente y segura reduce el tiempo de inactividad y mejora la productividad del personal, lo que se traduce en una gestión más efectiva. Todo ello contribuye a un desarrollo económico local más sólido y una administración pública orientada a resultados con un uso racional y estratégico de sus recursos digitales.

d) Justificación tecnológica

La implementación de un sistema de gestión de seguridad de la información en la Municipalidad Distrital de Végueta representa un avance tecnológico esencial para fortalecer la infraestructura digital institucional. En un contexto donde las tecnologías de la información son fundamentales para la operatividad y eficiencia de los gobiernos locales, contar con redes LAN de alta calidad y debidamente protegidas permite optimizar el desempeño de los servicios municipales. Este enfoque tecnológico garantiza la integridad, confidencialidad y disponibilidad de la información, reduce vulnerabilidades frente a amenazas cibernéticas y asegura la continuidad de los servicios ante posibles fallos del sistema. Además, promueve la interoperabilidad entre áreas municipales, facilita la automatización de procesos y contribuye al desarrollo de una gestión pública moderna, segura y alineada con las exigencias de la transformación digital.

1.3. Delimitaciones del estudio

a. Delimitación temporal

Esta investigación es de actualidad, por cuanto Sistema de gestión de seguridad de la información y la calidad de servicio de las redes LAN en la Municipalidad Distrital de Végueta, Huaura son vigentes.

b. Delimitación espacial

Esta investigación estuvo comprendida dentro de la Municipalidad Distrital de Végueta, Huaura.

c. Delimitación cuantitativa

Esta investigación se efectuó con una muestra censal y el procesamiento estadígrafo correspondiente.

d. Delimitación conceptual

Esta investigación abarco dos conceptos fundamentales: Sistema de gestión de seguridad de la información y la calidad de servicio de las redes LAN.

CAPÍTULO II. MARCO TEÓRICO

2.1. Antecedentes de la investigación

2.1.1. Antecedentes internacionales

Orellana (2022) en su tesis titulada: "Elaboración de una guía de implementación de un SGSI para la Corporación Ecuatoriana para el Desarrollo de la Investigación y la Academia - CEDIA". Realizada con el apoyo de la Universidad Politécnica Salesiana. El objetivo fue elaborar una guía de implementación de un SGSI para la Corporación Ecuatoriana para el desarrollo de la investigación y la academia - Cedia enfocado en la norma ISO/IEC 27002:2013. La metodología fue descriptiva, cuantitativa y cualitativa; su instrumento fue, cuestionarios, entrevistas y la observación directa de la situación actual de la empresa. La conclusión fue que Se puede concluir que seguridad de la información no solo se refiere a ciberseguridad o seguridad informática, puesto que un SGSI abarca tanto ese tipo de información como la que se encuentra en formato físico y de todas las áreas de la organización. CEDIA cuenta con activos muy importantes como cualquier organización, mismos que pueden estar expuestos a riesgos, los cuales no se reducen provocarían un gran problema dentro de la organización. • Para reducir los riesgos se debe implementar una metodología de análisis de riesgo, en este caso se analizó la metodología de la ISO/IEC 27001, puesto que cuenta con la evaluación y tratamientos de riesgos.

Espinoza (2022) en su tesis titulada: "Propuesta de diseño de un Sistema de Gestión de Seguridad de la Información para las Áreas de Educación y Protección Social de la Fundación Tierra Nueva con base en la norma internacional ISO/IEC 27001:2013". Realizada con el apoyo de la Universidad Politécnica Salesiana. El objetivo fue diseñar un Sistema de Gestión de Seguridad de la Información para las Áreas de Educación y Protección Social de la Fundación Tierra Nueva con base en la norma internacional ISO/IEC 27001:2013. La metodología fue descriptiva, cuantitativa y cualitativa; su instrumento fue, cuestionarios y entrevistas. La conclusión fue que, con la ejecución del diagnóstico realizado a las áreas de Educación y Protección Social de la Fundación Tierra Nueva, se determinó la no existencia de un Sistema de Gestión de Seguridad de la

Información, lo cual permitió el planteamiento de la propuesta del mismo para que las áreas mencionadas empiecen a manejar su información de manera segura y con base en la norma ISO/IEC 27001 para lograr si lo desean una certificación a futuro.

Quinapallo (2024) en su tesis titulada: "Procedimiento de control de información registrada en los formularios de inclusión del Estándar común de reporte". Realizada con el apoyo de la Universidad Tecnológica Israel. El objetivo fue rediseñar el procedimiento de control y análisis de la información registrada en los formularios CRS, en las aperturas de cuenta de la cooperativa, partiendo del desarrollo de los procesos actuales y la normativa vigente, para minimizar riesgos operativos e implementar controles adicionales por los departamentos o áreas supervisoras. La metodología fue descriptiva, cuantitativa y cualitativa; su instrumento fue, cuestionarios, entrevistas y observación. La conclusión fue que una vez analizado y fundamentado el marco normativo y técnico del Common Reporting Standard (CRS) ha proporcionado una comprensión profunda de los fundamentos técnicos del intercambio automático de información. La investigación permitió determinar que existen 3022 casos que tienen varias deficiencias por errores operativos en el registro de la información de los formularios CRS. Estas deficiencias incluyen el ingreso incorrecto del NIF, errores en la vinculación de los poderes extranjeros, ausencia de impresión de formularios CRS, ingreso de caracteres especiales en el campo NIF no permitidos.

Cando y Morales (2020) en su tesis titulada: "Implementación de una red LAN con acceso WAN, en la empresa GMS, administrada de acuerdo con la norma establecida por el Instituto SANS - SysAdmin Audit, Networking and Security Institute". Realizada con el apoyo de la Universidad Tecnológica Israel. El objetivo fue implementar una red LAN con acceso WAN, en la empresa GMS, administrada de acuerdo con los 20 controles establecidos por el Instituto SANS - SysAdmin Audit, Networking and Security Institute. La metodología fue enfoque metodológico mixto; su instrumento fue, cuestionarios, entrevistas y observación. La conclusión fue que se implementó una red LAN con acceso WAN, en la empresa GMS, administrada de acuerdo con los 20 controles establecidos por el Instituto SANS – SysAdmin, Networking and Security

Institute, la solución que se aplica en la red dentro del proyecto cumple con un diseño basado en el estándar de controles propuestos por el Instituto SANS, estos controles hacen cumplir con los principios de confidencialidad, integridad y disponibilidad, así también considera una implementación escalable, modular y de fácil administración.

Valenzuela (2020) en su tesis titulada: "Análisis y propuesta de mejoras a la infraestructura y seguridad de la red LAN de la empresa SICCEC para perfeccionar la disponibilidad de sus servicios". Realizada con el apoyo de la Universidad Politécnica Salesiana. El objetivo fue analizar y proponer un proyecto de mejoras a los problemas de seguridad e infraestructura de red LAN de la empresa SICCEC, para mejorar la disponibilidad de los principales servicios que maneja. La metodología fue descriptiva, cuantitativa y cualitativa; su instrumento fue, cuestionarios y observación. La conclusión fue que el recolectar información del estado actual de la red junto con el análisis de los perfiles de usuario, ayudó a determinar las herramientas y reglas que fueron implementadas de acuerdo a los requerimientos de la empresa, con el fin de solucionar los inconvenientes de seguridad y mejorar la disponibilidad de los servicios. La implementación de la virtualización en el nuevo servidor de SICCEC fue bastante útil, ya que solucionó uno de los mayores inconvenientes al implementar uno o más servicios dentro de un mismo servidor físico, con una correcta administración de las máquinas virtuales, monitoreo constante y correcto manejo de recursos de procesamiento en una solución libre como es XenServer.

2.1.2. Antecedentes nacionales

Galindo (2022) en su tesis titulada: "Sistema de gestión de seguridad de la información y su relación con la calidad de servicio de las redes LAN en la Municipalidad Distrital de Ilabaya". Realizada con el apoyo de la Universidad Privada De Tacna. El objetivo fue determinar la relación entre el SGSI y la calidad de servicio de las redes LAN en la Municipalidad Distrital de Ilabaya. La metodología fue enfoque cuantitativo donde se aplicó herramientas de recolección de datos, el tipo de investigación que se planteó para el desarrollo es aplicado de características descriptivas y correlacionales no experimenta; la población muestral fueron 63 personas comprendidos por funcionarios y empleados

públicos, su instrumento fue, cuestionario. La conclusión fue que para el contraste de correlación de Pearson se determinó que el valor hallado del coeficiente de correlación fue r = 0,540 (valor de p = 0,000); por lo tanto, existe una influencia directa y significativa entre el SGSI y la Calidad de Servicio de la Red LAN de la Municipalidad Distrital de Ilabaya. Quiere decir que existe una relación directa y significativa entre el SGSI y la Calidad de Servicio de las redes LAN en la Municipalidad Distrital de Ilabaya, es evidencia necesaria para el inicio de la implementación de un SGSI, lo cual se planteó al área encargada el diseño de SGSI iniciando con un análisis situacional de la entidad posteriormente se desarrolló políticas y controles de seguridad para la Municipalidad distrital de Ilabaya.

Suazo (2024) en su tesis titulada: “Sistema de gestión de seguridad de la información y la calidad de servicio de las redes en la Empresa Cerámica Lima S.A. - 2023”. Realizada con el apoyo de la Universidad Nacional José Faustino Sánchez Carrión. El objetivo fue determinar la relación que existe entre el sistema de gestión de seguridad de la información y la calidad de servicio de las redes en la empresa Cerámica Lima S.A. – 2023. La metodología fue el método deductivo, es una investigación aplicada, es de diseño no Experimental, tipo transversal, la investigación es de nivel correlacional; la muestra lo conformaron 265 trabajadores de la población, su instrumento fue, cuestionario. La conclusión fue que el modelo de correlación de Rho de Spearman devuelve un coeficiente de 0,142 y una significancia de 0,020 por lo que se puede comprobar, con un 95% de probabilidad, que existe una correlación positiva baja entre el sistema de gestión de seguridad de la información y la calidad de servicio de las redes en la empresa Cerámica Lima S.A. en el 2023.

Martínez (2023) en su tesis titulada: “Sistema de gestión de seguridad de la información y calidad del servicio del colegio Carlos A. Velásquez Ilo”. Realizada con el apoyo de la Universidad José Carlos Mariátegui. El objetivo fue establecer cuál será la correlación entre un SGSI y la calidad del servicio del colegio Carlos A. Velásquez Ilo. La metodología fue diseñada cuantitativamente bajo el diseño descriptivo de transcripción no experimental; la población conformada por del colegio Carlos A. Velásquez fue de 42 miembros, su instrumento fue,

cuestionario. La conclusión fue que se verifico que, si existe una coherencia entre las variables de SGSI y la calidad del servicio, accediendo a plantear los problemas de seguridad en la información, todo esto para mejorar sus procesos de la mano con la normativa ISO 27001, lo cual mejorará en minimizar la perdida de información. Así mismo se observó que el personal tenía poco conocimiento en cuanto ciberseguridad. Además, al identificar los principios de S.I. en correlación a la calidad del servicio del colegio Carlos A. Velásquez Ilo fue implantar orientaciones en la S.I de los sistemas que maneja el colegio.

Calcina (2023) en su tesis titulada: "Diseño, optimización, implementación e integración de las redes LAN administrativa e industrial, para mejorar la calidad de servicio con tecnología cisco en la Unidad Minera San Rafael 2021". Realizada con el apoyo de la Universidad Nacional Del Altiplano. El objetivo fue diseñar, optimizar, implementar e integrar las redes LAN administrativa e industrial para mejorar la calidad de servicio con tecnología Cisco en la Unidad Minera San Rafael 2021. La metodología fue el enfoque de investigación: se ajusta al tipo cuantitativo no experimental de corte transversal. Método de investigación hipotético-inductivo; la población de estudio está conformada por los tiempos de respuesta y las latencias, su instrumento fue, cuestionario y la ficha de revisión normativa. La conclusión fue que se diseñó e implementó una nueva red, luego, se comprobó la mejora de la calidad de servicio a través del diseño, implementación e integración de una nueva red LAN con tecnología CISCO en la Unidad Minera San Rafael, para ello se utilizó la prueba de diferencias de medias, donde se obtuvo que los tiempos de respuesta y latencias con la nueva red LAN son significativamente menores a la red anterior (en el nivel de significancia del 0.05).

Avalos (2020) en su tesis titulada: "Migración de DNS y DHCP para la mejora de servicios en las redes Lan del grupo de tiendas Retail en el Perú – 2020". Realizada con el apoyo de la Universidad Tecnológica del Perú. El objetivo fue realizar la migración y mejora de servicios de alto requerimiento en las redes LAN de grupo de empresas Retail en Perú. La metodología fue aplicada de nivel descriptivo - correlacional, utilizando un diseño no experimental; y la recolección de datos, su instrumento fue, cuestionario. La conclusión fue que la administración

es mucho más sencilla y fácil de manejar, siendo lo más importante, la correcta gestión de las asignaciones de las ips, lo cual nos permite ahorrar tiempo en el diagnóstico y anticiparnos a cualquier inconveniente. El proyecto ha ayudado a diagnosticar con mayor rapidez y tener un mayor control de los servicios, lo cual lo hemos visto reflejado en la disminución del tiempo de atención en la base de datos semanal. El tener una arquitectura redundante en diferentes data centers, nos permite tener el respaldo que necesitamos ante cualquier problema físico ya ocurrido.

2.2. Bases teóricas

2.2.1. Sistema de gestión de seguridad de la información (X)

Según Trujillo (2020) menciona que

> SGSI es un sistema de gestión de seguridad de la información quien tiene como responsabilidad proporcionar varios procesos y herramientas basados en el estándar ISO27001, esta norma permite a diferentes organizaciones o entidades identificar las debilidades con respecto a la seguridad de la información, guiando al usuario para una eficaz administración de los riesgos identificados.

Según Ccesa, (2017), indica que

> Un sistema de gestión de seguridad de la información se define como un conjunto de procesos que permite a una organización o entidades establecer, implementar, mantener y mejorar continuamente la seguridad de la información de acuerdo con los riesgos que se enfrenta, también mencionan la configuración preestablecida de la configuración asumida del SGSI. Procesos formales y definiciones claras de responsabilidades basadas en un conjunto de políticas, planes y procedimientos que deben incorporarse.

La información es altamente reveladora porque depende de factores internos y externos; los autores concluyeron que la información es considerada como uno de los activos más relevantes e importante, y se le debe dar especial cuidado y protección, pues sin ella sería explotada por los ciberdelincuentes a nivel mundial afectando a todo tipo de sectores públicos y privado (Diaz, 2021)

Según Alvarado, (2022) menciona que

> Un SGSI consiste en el conjunto de políticas, procedimientos y directrices junto a los recursos y actividades asociados que son administrados colectivamente por una organización, en la búsqueda de proteger sus activos de información esenciales. A continuación, hablaremos de qué significan cada uno de estos términos en relación con la información.

Si hablamos de seguridad de la información utilizando la norma ISO 2700, se basa en todos los procedimientos necesarios para proteger la información, mantenimiento, prevención, centrándose en la confidencialidad, asegurando que la información esté completa y disponible ante cualquier riesgo que pueda surgir. Destruirlo desde fuera o desde dentro (Castro, 2014).

Tenemos que tener en cuenta que para evitar pérdidas económicas y tiempo en una empresa y/o organización, debemos mantener la información y la integridad del sistema informático, sin olvidar el riesgo que puede ocasionar el acceso ajeno de usuarios no autorizados que entren al sistema (García A, et al, 2011).

Según Castro (2018)

> El sistema de gestión de seguridad de la información es un conjunto de elementos interrelacionados o que interactúan en cuanto a estructura organizacional, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos utilizados por una organización para establecer políticas y objetivos de la seguridad de la información. También indica que la implementación de un sistema de gestión de la seguridad de la información se basa en la norma ISO 27001, utilizando el ciclo Deming el cual permite implantar un plan de mejora continua. El ciclo Deming tiene las siguientes etapas:
>
> **Planificar:** Castro (2018) indica que en esta etapa se define el alcance y la política de seguridad, empezando con un análisis de riesgo para conocer el estado actual de la entidad, define un plan de tratamiento de información y de riesgos, para seguir con la implementación de controles para los diversos riesgos que la administración no está tomando en cuenta. 16

Hacer: Castro (2018) indica que en esta etapa del ciclo Deming o ciclo PDCA se centra en la planificación de los tratamientos de riesgos, esto influye a la concientización de los usuarios, y la definición de métricas para los distintos controles que se van a aplicar.

Verificar: Castro (2018) indica que en esta etapa incluye la realización de auditorías para verificar la correcta implementación del sistema de gestión de la seguridad de la información, la realización de auditorías internas y la gestión general de la empresa.

Actuar: Castro (2018) indica que en esta etapa se revisa el resultado de la auditoria y se debe tomar diversas acciones correctivas, preventivas o de mejora

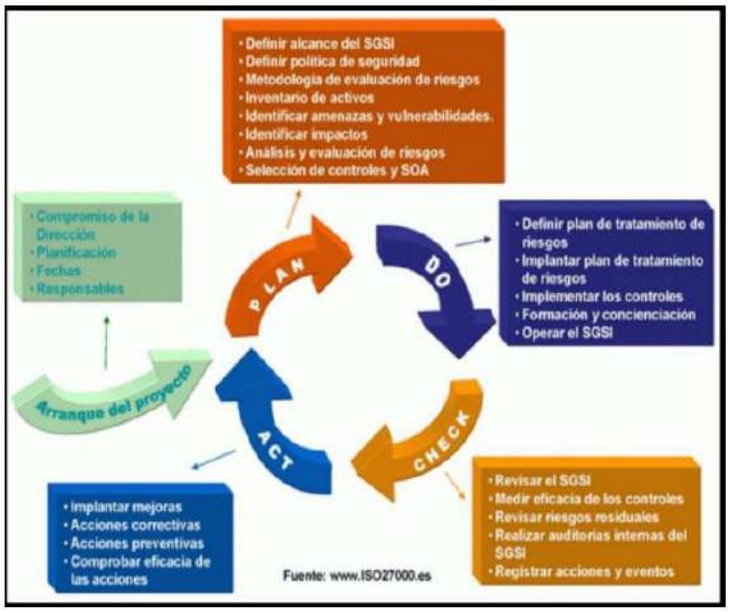


Figura 1. Ciclo Deming o PDCA

Calder y Watkins (2010) explican que

> Un sistema de gestión de seguridad de la información proporciona a las organizaciones un marco estructurado que permite identificar, analizar y gestionar los riesgos que afectan la confidencialidad, integridad y disponibilidad de la información. Además, señalan que estos sistemas deben estar alineados con los objetivos estratégicos de la entidad, asegurando la implementación continua de políticas, procedimientos y controles adaptados a las necesidades del entorno organizacional.

Según la norma ISO/IEC 27001 (2013),

> Un sistema de gestión de seguridad de la información se basa en la adopción de un enfoque sistemático y continuo que tiene por finalidad proteger la información mediante el tratamiento adecuado de los riesgos asociados. Este sistema establece los requisitos para planificar, implementar, monitorear, revisar y mejorar las prácticas de seguridad de la información en una organización, proporcionando confianza a las partes interesadas sobre la gestión eficaz de los riesgos.

Whitman y Mattord (2011) afirman que

> El sistema de gestión de seguridad de la información representa una herramienta esencial para lograr una administración efectiva de los activos informáticos. Este sistema permite establecer responsabilidades claras, coordinar procesos de evaluación de amenazas y vulnerabilidades, y definir medidas preventivas y correctivas que garanticen la protección integral de los datos. En este contexto, el SGSI se convierte en un instrumento clave para la gobernanza tecnológica y la toma de decisiones basada en riesgos.

2.2.1.1. Seguridad confidencial

Según Calder y Watkins (2012), define que

> La confidencialidad de la información es un principio esencial del sistema de gestión de seguridad de la información, ya que busca asegurar que los datos sensibles solo sean accesibles para las personas autorizadas. Este principio se aplica mediante mecanismos como la autenticación, la encriptación, el control de accesos y políticas de clasificación de la información. Si se compromete la confidencialidad, no solo se pone en riesgo la privacidad, sino también la integridad de los procesos y la imagen institucional de la organización. (p. 83)

Además, Humphreys (2008), define que

> Dentro del marco del sistema de gestión de seguridad de la información, la confidencialidad se refiere a la protección de la información frente a accesos no autorizados, tanto internos como

externos. Esto implica establecer políticas claras de manejo de datos, implementar controles técnicos y administrativos, y fomentar una cultura de seguridad entre los empleados. La pérdida de confidencialidad puede generar daños económicos, pérdida de competitividad, sanciones legales y la desconfianza de los clientes y partes interesadas (p.56).

Solms y Niekerk, (2011), menciona que

> Garantizar la confidencialidad de la información es uno de los objetivos fundamentales de cualquier sistema de gestión de seguridad. La información debe estar protegida de forma que solo puedan acceder a ella quienes tienen el derecho y la necesidad de hacerlo. Esto requiere una combinación de medidas tecnológicas, como la encriptación de datos y el uso de firewalls, junto con políticas organizacionales estrictas. Cuando la confidencialidad se ve comprometida, la organización se expone a amenazas internas, fraudes, espionaje industrial y violaciones legales que pueden impactar gravemente en su continuidad operativa (p. 93).

2.2.1.1.1. Acceso restringido a la información

El control de accesos basado en roles garantiza que solo las identidades autorizadas puedan interactuar con los recursos sensibles, estableciendo permisos granulares y revisiones periódicas para prevenir escaladas de privilegios y filtraciones inadvertidas de datos críticos (Whitman y Mattord, 2010, p. 145).

Definir políticas estrictas de acceso asegura que cada usuario solo reciba los permisos necesarios para sus funciones, reforzado con autenticación multifactor y auditorías de privilegios, lo que minimiza el riesgo de accesos no autorizados y posibles brechas de confidencialidad (Tipton y Krause, 2007, p. 302).

La segmentación de usuarios mediante perfiles y la aplicación de controles de acceso lógicos y físicos constituyen la primera línea

de defensa en un SGSI, ya que previenen la exposición de información crítica a personal no autorizado y facilitan la trazabilidad de eventos (Calder y Watkins, 2012, p. 68).

2.2.1.1.2. Uso de contraseñas seguras

Implementar políticas de complejidad y caducidad de contraseñas obliga a los usuarios a generar credenciales resistentes a ataques de fuerza bruta y diccionario, reduciendo significativamente la probabilidad de compromiso de cuentas y la exposición de datos confidenciales (Tipton y Krause, 2007, p. 336).

Almacenar contraseñas en repositorios cifrados y aplicar hashing fuerte con sal protege las credenciales frente a filtraciones de bases de datos y ataques de ingeniería inversa, garantizando que incluso si un repositorio es comprometido, las contraseñas no serán fácilmente reveladas (Pfleeger y Pfleeger, 2012, p. 290).

La combinación de requisitos de longitud mínima, mezcla de caracteres y expiración periódica de contraseñas, unida a la concienciación del usuario sobre buenas prácticas, es fundamental para mantener la confidencialidad, ya que las credenciales débiles representan uno de los vectores de ataque más utilizados (Whitman y Mattord, 2010, p. 146).

2.2.1.1.3. Control de usuarios y roles

Asignar roles basados en principios de menor privilegio y revisar periódicamente los perfiles de usuario asegura que cada actor disponga solo de los accesos indispensables, evitando acumulación de permisos innecesarios y reduciendo la superficie de ataque (Humphreys, 2008, p. 79).

La definición clara de responsabilidades y la separación de funciones críticas impiden conflictos de interés y fraudes internos, al garantizar que ninguna persona controle de forma exclusiva

procesos sensibles sin supervisión ni controles independientes (Calder y Watkins, 2012, p. 68).

Integrar la gestión de identidades con directorios centralizados permite automatizar altas, bajas y modificaciones de usuarios, asegurando que los derechos de acceso se ajusten dinámicamente a cambios de rol y evitando accesos obsoletos o inapropiados (Solms y Niekerk, 2011, p. 71).

2.2.1.2. Seguridad integral

Según Whitman y Mattord, (2010), define que

> La seguridad integral no puede limitarse solo al ámbito tecnológico. Debe integrar la seguridad física, lógica, organizacional y humana como un conjunto interdependiente. En un SGSI, este enfoque permite prevenir brechas que podrían originarse no solo por vulnerabilidades técnicas, sino también por malas prácticas, errores humanos o fallos en la infraestructura. Solo una gestión coordinada puede garantizar que todos los activos estén adecuadamente protegidos. (p. 132).

Además, Tøndel, et al. (2014), define que

> En el marco de la gestión de seguridad de la información, la seguridad integral se entiende como la articulación de políticas, procesos y tecnologías que trabajan en conjunto para proteger la totalidad de los recursos informáticos. No se trata únicamente de asegurar la información digital, sino de resguardar toda la estructura que la sustenta, incluyendo el entorno físico y humano, mediante una visión sistémica y permanente. (p. 58).

Tipton y Krause, (2007), menciona que

> Un sistema de gestión de seguridad eficaz se basa en el concepto de seguridad integral, en el cual los riesgos se analizan y se mitigan desde una perspectiva global. Esto incluye el análisis de amenazas internas y externas, técnicas y humanas, planificando respuestas

adecuadas para cada una de ellas. La seguridad no debe implementarse como elementos separados, sino como un sistema interrelacionado que actúe de forma coherente ante cualquier incidente (p. 249).

2.2.1.2.1. Verificación de integridad

Aplicar algoritmos de hashing criptográfico como SHA-256 y generar sumas de comprobación periódicas permite detectar cualquier alteración no autorizada de archivos o bases de datos, garantizando que los datos almacenados permanezcan intactos y sin modificaciones maliciosas (Pfleeger y Pfleeger, 2012, p. 224).

La verificación de integridad debe incluir tanto datos en reposo como en tránsito, con mecanismos de firma digital y control de versiones que registren cada cambio, de forma que se pueda reconstruir el historial de documentos y detectar manipulaciones indebidas (Solms y Niekerk, 2011, p. 121).

Incorporar registros de control que documenten cada comprobación de integridad y alerten automáticamente sobre discrepancias fortalece la capacidad forense del SGSI, ya que proporciona evidencia de cualquier intento de corrupción o alteración de la información (Tanenbaum y Wetherall, 2014, p. 412).

2.2.1.2.2. Registro de cambios

Mantener bitácoras detalladas de todas las modificaciones en archivos y configuraciones, con información de quién, cuándo y qué cambió, facilita la auditoría y la investigación de incidentes, permitiendo la rápida identificación de responsables y la restauración de estados previos (Humphreys, 2008, p. 79).

Los sistemas de gestión de registros deben garantizar la inmutabilidad de los logs y su almacenamiento seguro, de modo que no puedan ser alterados por usuarios maliciosos, asegurando

así la confiabilidad de la información de auditoría (Calder y Watkins, 2012, p. 101).

Integrar soluciones de SIEM para centralizar y correlacionar registros de diferentes sistemas permite generar alertas en tiempo real sobre actividades anómalas y garantizar que los registros de cambios sean completos, coherentes y estén siempre disponibles para análisis posteriores (Tipton y Krause, 2007, p. 249).

2.2.1.2.3. Prevención de modificaciones no autorizadas

Implementar mecanismos de control de versiones y bloqueo de archivos impide que múltiples usuarios editen simultáneamente, evitando inconsistencias de datos y asegurando que cualquier intento de alteración no autorizada sea inmediatamente detectado y bloqueado (Solms y Niekerk, 2011, p. 121).

Utilizar firmas digitales en documentos críticos garantiza que cualquier cambio no autorizado quede invalidado, ya que la firma se anula al alterarse el contenido, proporcionando un método fiable de prevención de manipulaciones (Pfleeger y Pfleeger, 2012, p. 224).

La implementación de sistemas de detección de integridad en tiempo real, que comparan hashes calculados al vuelo con valores de referencia, fortalece la prevención de alteraciones, alertando inmediatamente al equipo de seguridad ante cualquier discrepancia (Humphreys, 2008, p. 34).

2.2.1.3. Disponibilidad operativa

Según Pfleeger y Pfleeger, 2012), define que

> La disponibilidad operativa en un sistema de gestión de seguridad de la información se refiere a garantizar que los usuarios autorizados puedan acceder a los recursos y servicios cuando los necesiten, minimizando tiempos de inactividad y asegurando que las

> infraestructuras críticas permanezcan operativas incluso ante fallos, ataques o desastres, mediante estrategias de redundancia y recuperación ante incidentes. (p. 112).

Además, Peltier, (2005), define que

> Dentro del SGSI, la disponibilidad operativa implica no solo la implementación de copias de seguridad y planes de recuperación, sino también el monitoreo continuo de los sistemas, la gestión proactiva de parches y actualizaciones, y la planificación de capacidad. Esto asegura que los servicios críticos permanezcan accesibles y con el rendimiento adecuado, incluso ante picos de demanda o eventos imprevistos. (p. 78).

Harris, (2013), menciona que

> La disponibilidad operativa es uno de los tres pilares fundamentales de la seguridad de la información y se logra mediante la integración de controles técnicos —como balanceadores de carga, clustering y sistemas de alimentación ininterrumpida— con procedimientos organizativos que incluyen planes de continuidad del negocio y pruebas periódicas de recuperación, garantizando así un nivel de servicio acordado con los usuarios (p. 146).

2.2.1.3.1. Tiempo de disponibilidad de los sistemas

El porcentaje de disponibilidad se calcula midiendo el tiempo en que los sistemas permanecen operativos frente al total del periodo evaluado, siendo esencial para verificar el cumplimiento de acuerdos de nivel de servicio y justificar inversiones en redundancia y alta disponibilidad (Tanenbaum y Wetherall, 2014, p. 412).

Para mantener alta disponibilidad es necesario diseñar arquitecturas redundantes de servidores y enlaces, acompañadas de balanceadores de carga que distribuyan el tráfico y eviten puntos

únicos de fallo que puedan causar interrupciones prolongadas (Pfleeger y Pfleeger, 2012, p. 112).

Monitorear la disponibilidad mediante sistemas de supervisión proactiva y alertas automatizadas permite identificar y resolver problemas antes de que afecten al usuario final, reduciendo significativamente los tiempos de inactividad no planificada (Peltier, 2005, p. 78).

2.2.1.3.2. Planes de recuperación ante desastres

Los planes de recuperación ante desastres documentan procedimientos detallados para restaurar servicios críticos tras cortes de energía, fallos de hardware o desastres naturales, e incluyen pruebas periódicas que validan la eficacia y tiempos de recuperación definidos (Peltier, 2005, p. 142).

Incluir simulacros de recuperación y ejercicios de conmutación por error en entornos de prueba permite medir el tiempo real de restauración y ajustar procedimientos para cumplir los objetivos de tiempo de recuperación establecidos en el SGSI (Harris, 2013, p. 146).

Integrar soluciones de replicación síncrona y asíncrona de datos en sitios secundarios garantiza que, ante un incidente mayor, la organización pueda cambiar operaciones con mínima pérdida de información y dentro de los plazos acordados (Pfleeger y Pfleeger, 2012, p. 295).

2.2.1.3.3. Mantenimiento periódico de infraestructura

Programar ventanas de mantenimiento preventivo para actualizar firmware, parches de seguridad y comprobaciones de hardware reduce la probabilidad de fallos inesperados y contribuye a mantener la disponibilidad operativa de los sistemas (Harris, 2013, p. 359).

> Documentar y seguir procedimientos estandarizados de mantenimiento, incluidos checklists y registros de acciones realizadas, garantiza que cada intervención sea consistente y permita rastrear el historial de cambios en la infraestructura (Peltier, 2005, p. 82).

> Monitorear métricas de salud de hardware y temperatura, así como el estado de baterías en sistemas de alimentación ininterrumpida, ayuda a anticipar fallos físicos antes de que interrumpan el servicio, optimizando los esfuerzos de mantenimiento (Tanenbaum y Wetherall, 2014, p. 423).

2.2.1.4. Cumplimiento normativo

Según Calder y Watkins, (2012), define que

> El cumplimiento normativo en un SGSI implica no solo la adopción de estándares internacionales como la serie ISO/IEC 27000, sino también la alineación con las leyes, regulaciones y políticas internas de la organización. Este enfoque holístico obliga a las entidades a desarrollar procedimientos de auditoría, establecer controles documentados y mantener evidencia de conformidad para demostrar responsabilidad legal y operativa ante autoridades y partes interesadas. (p. 152).

Además, Humphreys, (2008), define que

> Garantizar el cumplimiento normativo dentro de un sistema de gestión de seguridad de la información requiere implementar un marco de controles que verifique el apego a las obligaciones legales, contractuales y reglamentarias. Esto incluye la identificación continua de requisitos aplicables, la evaluación periódica de brechas, la formalización de políticas de seguridad y la ejecución de auditorías internas y externas para certificar la conformidad (p. 114).

Von Solms y von Solms (2004), menciona que

> El cumplimiento normativo es un pilar fundamental de la gobernanza de la seguridad de la información. Un SGSI eficaz debe integrar procesos que aseguren la conformidad continua con marcos legales, regulatorios y contractuales, soportados por actividades de revisión, actualización de políticas y formación de personal. Solo así se mitigan riesgos de sanciones, pérdidas patrimoniales y daños reputacionales derivados de incumplimientos (p. 87).

2.2.1.4.1. Adopción de normativas

Adoptar estándares como ISO/IEC 27001 requiere documentar políticas, procedimientos y controles, e incorporar la mejora continua mediante el ciclo Plan-Do-Check-Act, lo que asegura la alineación con las mejores prácticas internacionales y la responsabilidad legal (Calder y Watkins, 2012, p. 152).

La adopción de marcos regulatorios obligatorios y recomendaciones internacionales obliga a las organizaciones a identificar requisitos legales aplicables, evaluar brechas y establecer planes de acción que demuestren conformidad ante auditorías internas y externas (Humphreys, 2008, p. 114).

Integrar normativas sectoriales y contractuales en el SGSI garantiza que los procesos diarios cumplan con obligaciones regulatorias específicas, reduciendo riesgos de sanciones y fortaleciendo la confianza de clientes y socios comerciales (von Solms y von Solms, 2004, p. 87).

2.2.1.4.2. Auditorías de seguridad de la información

Realizar auditorías internas programadas permite verificar la eficacia de los controles del SGSI, identificar no conformidades y establecer acciones correctivas antes de auditorías de certificación, asegurando el cumplimiento continuo de la norma ISO/IEC 27001 (Humphreys, 2008, p. 118).

Auditorías externas independientes aportan una visión objetiva sobre la madurez del SGSI, evaluando la documentación, la implementación de controles y la cultura de seguridad, y generando informes que guían la mejora continua (Calder y Watkins, 2012, p. 153).

Integrar hallazgos de auditorías en el ciclo de gestión de riesgos permite priorizar las no conformidades según su criticidad, optimizar recursos y demostrar ante las partes interesadas un compromiso real con el cumplimiento normativo (Tipton y Krause, 2007, p. 338).

2.2.1.4.3. Políticas de seguridad implementadas

Formalizar políticas de seguridad y mantenerlas actualizadas, aprobadas por la alta dirección y difundidas a todo el personal, es requisito para demostrar que la organización conoce y aplica sus obligaciones legales y contractuales en materia de seguridad (von Solms y von Solms, 2004, p. 89).

La existencia de políticas escritas, claras y accesibles, acompañadas de procedimientos asociados, facilita la estandarización de prácticas, la capacitación del personal y la evaluación del cumplimiento operativo de los requisitos del SGSI (Humphreys, 2008, p. 56).

Documentar y divulgar políticas de seguridad fortalecidas por controles de gobernanza, revisiones periódicas y sanciones por incumplimiento crea un entorno donde la responsabilidad y la conformidad son medibles y sujetas a mejora continua (Calder y Watkins, 2012, p. 152).

2.2.2. La calidad de servicio de las redes LAN (Y)

Según Ley et. al, (2021) señala que

> Una LAN se considera un recurso técnico eficiente que permite el intercambio de información entre dispositivos informáticos interconectados: es un grupo de dispositivos interconectados físicamente, como una oficina corporativa o una habitación en una casa; pueden ser grandes o pequeños, que puede ser un solo usuario conectado a una red doméstica, o miles de personas conectadas a una empresa, organización, institución o red corporativa.

De acuerdo Cacuango (2019) señala que

> La calidad de servicio en una red administra y controla los parámetros de varios flujos de tráfico, como audio, video y datos digitales (software, documentos, base de datos y archivos), así como también controla la provisión de servicios a medida que viajan a través de la red, para que se pueda proporcionar información precisa a los usuarios sin perder información o datos.

Además, Zheng (2017) señala que

> Una red de datos que cubre un área geográfica pequeña y limitada, conectando estaciones de trabajo, terminales o equipos en edificios, oficina o campus, una red LAN incluye computadoras, periféricos, dispositivos de red y tarjetas de interfaz de red (NIC). Proporciona conectividad las 24 horas del día, los 7 días de la semana y utilizan los estándares de la capa física y la capa de enlace de datos del modelo OSI, Ethernet, FDDI y Token Ring son las tecnologías LAN más populares, aunque el estándar más utilizado es Ethernet. El estándar Ethernet es la conectividad más segura y estable para las entidades públicas o privadas, garantizando una fluidez de datos estable y el intercambio de datos suele ser de manera inmediata. En la Figura 6 podemos observar cómo se interconectan computadoras, servidores, teléfono, impresora, fax, entre otros.

Según Berry, et al. (1989) detalla que “calidad de servicio es la conformidad de los usuarios receptores y realidad en la percepción, lo que los usuarios deseen es la preservación de la información mediante las dimensiones tangibilidad, confiabilidad, tiempo de respuesta, seguridad y empatía”.

En referencia a calidad de servicio de las redes LAN detalla que la calidad general de la gestión de red es evaluada mediante rigurosos criterios tales como importancia y significación de gestión de redes, eficacia y eficiencia, manejabilidad, interactividad, seguridad, calidad técnica general, acceso a la red, diseño y rendimiento (Universidad Rafael Belloso Chacín URBC, 2011).

Forouzan (2007) indica que

> La calidad de servicio en redes LAN está determinada por múltiples factores como el ancho de banda disponible, el retardo, la fluctuación de la demora y la pérdida de paquetes. Explica que, para lograr un alto nivel de calidad, se deben implementar mecanismos de priorización del tráfico, gestión de colas y monitoreo constante del rendimiento, lo cual es vital especialmente en redes con alta demanda y tráfico multimedia.

Tanenbaum y Wetherall (2011) señalan que

> En una red LAN, la calidad de servicio implica garantizar que todos los dispositivos conectados puedan transmitir y recibir datos de manera eficiente, sin interrupciones significativas. Subrayan que esto se logra mediante protocolos de control de congestión, esquemas de acceso al medio bien diseñados y arquitectura de red optimizada que reduzca los cuellos de botella.

Kurose y Ross (2013) argumentan que

> La calidad de servicio en una red LAN se refiere al nivel de rendimiento del sistema medido en términos de velocidad de transmisión, estabilidad de conexión y disponibilidad. Añaden que una buena calidad de servicio implica la implementación de políticas que controlen el tráfico, gestionen la congestión y garanticen la entrega puntual y segura de los datos, lo cual es esencial en entornos corporativos.

2.2.2.1. Velocidad de transmisión

Según Stallings, (2013), define que

> La velocidad de transmisión en una red LAN se define como la cantidad de bits que pueden enviarse satisfactoriamente por segundo a través del medio físico, medida típicamente en megabits por segundo (Mbps). Esta métrica es crítica para evaluar el rendimiento de aplicaciones sensibles al ancho de banda, como videoconferencias y transferencia de archivos de gran tamaño, y se ve afectada por factores como la topología, la calidad del cableado y la carga de tráfico concurrente. (p. 255).

Además, Kurose y Ross, (2013), define que

> El análisis de la velocidad de transmisión en LAN debe considerar tanto el rendimiento pico como el rendimiento sostenido. Mientras el rendimiento pico refleja la máxima capacidad teórica del enlace, el rendimiento sostenido muestra la tasa real observada durante periodos prolongados, la cual incorpora la sobrecarga de protocolos, colisiones en Ethernet y gestión de accesos. Esta distinción es fundamental para dimensionar correctamente la infraestructura de red y garantizar la experiencia de usuario (p. 120).

Tanenbaum y Wetherall, (2014), menciona que

> En el contexto de la calidad de servicio en LAN, la velocidad de transmisión se evalúa mediante herramientas de medición que registran el throughput efectivo, es decir, los bits de datos útiles recibidos por unidad de tiempo, descontando los bits de control y reenvío. Esta medición realista permite identificar cuellos de botella y planificar mejoras en el switching y en los mecanismos de priorización de tráfico (p. 387).

2.2.2.1.1. Tasa de transferencia de datos (Mbps)

La tasa de transferencia de datos en una red LAN representa el volumen de información que puede ser transmitido de forma confiable en un segundo. Este parámetro no solo depende del ancho

de banda teórico del medio, sino también de la eficiencia de los protocolos de enlace y de la calidad del cableado y los conectores usados en la infraestructura. (Stallings, 2013, p. 256)

Cuando se analiza la tasa de transferencia en redes locales, es fundamental diferenciar entre el throughput máximo la velocidad pico que la red puede alcanzar bajo condiciones ideales y el throughput efectivo, que es el volumen de datos útiles entregados al nivel de aplicación tras descontar encabezados, retransmisiones y otros datos de control. (Kurose y Ross, 2013, p. 121)

El análisis de la tasa de transferencia de datos requiere el uso de herramientas de medición especializadas que envían flujos de prueba y miden el volumen de bytes recibidos por segundo. Estos tests permiten identificar cuellos de botella, evaluar la capacidad de conmutación de los switches y dimensionar apropiadamente la red para las necesidades de tráfico concurrente. (Tanenbaum y Wetherall, 2014, p. 396)

2.2.2.1.2. Tiempo de respuesta de la red

El tiempo de respuesta se compone de varios componentes: retardo de propagación, retardo de transmisión, retardo de procesamiento y retardo de cola en los dispositivos. Su evaluación prolongada permite detectar congestiones y desajustes en los parámetros de Quality of Service (QoS) que afectan aplicaciones sensibles a la latencia, como VoIP y juegos en línea. (Stallings, 2013, p. 263)

Para medir el tiempo de respuesta en una LAN, se utilizan paquetes ICMP o flujos UDP de prueba, midiendo el round-trip time (RTT). Estos datos, agregados en intervalos regulares, muestran la variabilidad del retardo y ayudan a ajustar buffers y algoritmos de encolamiento en switches para garantizar un rendimiento consistente. (Peterson y Davie, 2007, p. 176)

El retardo de respuesta en redes LAN es crítico para aplicaciones interactivas. La métrica de one-way delay, que mide el tiempo de un solo sentido del paquete, se complementa con el jitter y la pérdida de paquetes para obtener un panorama completo de la experiencia de usuario, permitiendo optimizar parámetros de QoS a nivel de switch y router. (Kurose y Ross, 2013, p. 124)

2.2.2.1.3. Velocidad promedio de carga y descarga

La velocidad promedio de carga y descarga se calcula midiendo el throughput efectivo en intervalos prolongados, descontando retransmisiones y tráfico de control. Esta métrica revela la eficiencia real de la red y permite identificar desequilibrios entre tráfico ascendente y descendente, fundamentales para entornos de backup y sincronización de datos en la nube. (Tanenbaum y Wetherall, 2014, p. 397)

En pruebas de velocidad de carga y descarga, es común utilizar patrones de tráfico TCP para evaluar la capacidad de adaptarse a cambios de ventana de congestión y control de flujo. Los resultados ayudan a optimizar configuraciones de buffer y algoritmos de scheduling en los switches, mejorando la experiencia tanto en subida como en bajada. (Peterson y Davie, 2007, p. 199)

La evaluación de la velocidad promedio de carga y descarga mediante herramientas como iPerf o NetPerf proporciona un valor de throughput bidireccional. Estos valores, comparados con las especificaciones del fabricante de los equipos de red, permiten validar el rendimiento real de la planta física y de los protocolos de enlace implementados. (Kurose y Ross, 2013, p. 119)

2.2.2.2. Estabilidad de conexión

Según Stallings, (2013), define que

> La estabilidad de conexión en redes LAN se define como la capacidad de mantener un nivel constante de rendimiento y

> conectividad durante un periodo prolongado, sin variaciones significativas en el ancho de banda, la latencia o la pérdida de paquetes. Esta consistencia es vital para aplicaciones en tiempo real, como VoIP o video streaming, que requieren una entrega continua de dato. (p. 278).

Además, Kurose y Ross, (2013), define que

> En el análisis de la calidad de servicio de redes LAN, la estabilidad de conexión se evalúa mediante métricas como el porcentaje de paquetes perdidos, la variación de la latencia (jitter) y la frecuencia de reconexiones. Una red estable debe mostrar bajos niveles de jitter y pérdida de paquetes, así como una mínima fluctuación en el retardo de transmisión, garantizando así una experiencia de usuario uniforme (p. 144).

Peterson y Davie, (2007), menciona que

> La estabilidad de conexión se considera un componente esencial de la calidad de servicio, ya que refleja la fiabilidad de la red para mantener las sesiones activas sin interrupciones. Se mide a través de indicadores como el tiempo medio entre fallos de conexión, la tasa de reconexión automática y la consistencia en la entrega de tramas, factores que determinan la robustez de la infraestructura LAN frente a picos de carga y fluctuaciones de tráfico (p. 190).

2.2.2.2.1. Frecuencia de caídas de red por semana

La frecuencia de interrupciones en una LAN se mide contando cuántas veces la red pierde conectividad en un intervalo definido. Un número elevado de caídas semanales refleja problemas en la redundancia de enlaces, fallos en dispositivos o configuraciones erróneas de protocolos de spanning tree, lo que compromete la experiencia del usuario (Stallings, 2013, p. 278).

Contar las reconexiones necesarias tras pérdidas de enlace permite evaluar la eficacia de los mecanismos de recuperación

automática. Un alto recuento de caídas semanales indica deficiencias en el mantenimiento preventivo y en las políticas de gestión de fallos, factores críticos para garantizar la continuidad operativa (Peterson y Davie, 2007, p. 198).

La métrica de caídas por semana también sirve para dimensionar correctamente la infraestructura: si los enlaces redundantes no activan conmutación a tiempo o los switches tardan en relevar rutas, las interrupciones se suceden. Esto exige revisar tanto la topología como los tiempos de convergencia del protocolo (Tanenbaum y Wetherall, 2014, p. 389).

2.2.2.2.2. Fluctuación del ancho de banda

La variación del ancho de banda disponible en una LAN a lo largo del tiempo refleja la presencia de congestión o interferencias. Observar picos y caídas pronunciadas permite identificar momentos de sobrecarga en switches o colisiones frecuentes, lo que ayuda a planificar ampliaciones o ajustes en la configuración de QoS (Kurose y Ross, 2013, p. 146).

Monitorear la fluctuación de throughput efectivo, descontando retransmisiones y datos de control, ofrece un panorama real del rendimiento de la red. Cuando las variaciones superan ciertos umbrales, indican que es necesario revisar la calidad del cableado, la configuración de puertos o implementar mecanismos de shaping y policing (Stallings, 2013, p. 280).

La inconsistencia del ancho de banda impacta directamente en aplicaciones sensibles a la capacidad de enlace. Analizar valores de average, peak y burst throughput a diferentes horas y cargas de tráfico facilita la identificación de cuellos de botella y la optimización de políticas de encolamiento en los dispositivos de red (Peterson y Davie, 2007, p. 200).

2.2.2.2.3. Variación en el tiempo de respuesta

El jitter, o variación en el retardo de entrega de paquetes, se calcula midiendo el desvío estándar de los tiempos de ida y vuelta de múltiples muestras. Valores elevados de jitter comprometen la calidad de llamadas VoIP y video en tiempo real, por lo que su monitoreo continuo es esencial para ajustar buffers y políticas de scheduling (Stallings, 2013, p. 281).

Medir la variación en la latencia implica registrar el one-way delay y compararlo con el round-trip time promedio. Estos datos indican la consistencia del enlace y permiten detectar congestión intermitente, picos de tráfico o problemas en las tablas de enrutamiento que provocan retardos irregulares (Kurose y Ross, 2013, p. 144).

La estabilidad en el tiempo de respuesta se cuantifica también mediante el tiempo medio entre variaciones críticas, definido como el intervalo en el que el retardo cambia más de un porcentaje dado. Esta medida ayuda a planificar mejoras en hardware y a calibrar algoritmos de Quality of Service para minimizar la variabilidad (Peterson y Davie, 2007, p. 190).

2.2.2.3. Disponibilidad del servicio

Según Stallings, (2013), define que

> La disponibilidad del servicio en redes LAN se define como la capacidad de los sistemas y componentes de red para permanecer operativos y accesibles para los usuarios autorizados durante el tiempo acordado. Para garantizar altos niveles de disponibilidad, se emplean técnicas como redundancia de enlaces, clustering de dispositivos, sistemas de alimentación ininterrumpida y acuerdos de nivel de servicio que especifican tiempos máximos de inactividad permitida. (p. 266).

Además, Kurose y Ross, (2013), define que

> En el contexto de calidad de servicio, la disponibilidad del servicio se mide mediante indicadores como el tiempo medio entre fallos (MTBF), el tiempo medio de reparación (MTTR) y el porcentaje de tiempo de actividad (uptime) garantizado. Estos parámetros permiten evaluar la fiabilidad de la infraestructura LAN y planificar estrategias de recuperación y mantenimiento preventivo para reducir el impacto de interrupciones en las operaciones críticas (p. 198).

Tanenbaum y Wetherall, (2014), menciona que

> La disponibilidad del servicio es uno de los principales objetivos de la gestión de redes LAN, ya que influye directamente en la productividad del usuario y la continuidad del negocio. Para asegurar niveles de servicio óptimos, se implementan mecanismos de tolerancia a fallos, replicación de datos y balanceo de carga, además de realizar pruebas periódicas de conmutación por error y simulacros de recuperación ante desastres (p. 421).

2.2.2.3.1. Tiempo total de red operativa

El tiempo total de operatividad se calcula sumando las horas en que la LAN permanece accesible sin interrupciones. Esta métrica, expresada en horas o como porcentaje, permite verificar el cumplimiento de los acuerdos de nivel de servicio y detectar patrones de fallos recurrentes que requieran acciones de mejora (Peltier, 2005, p. 82).

Monitorear la disponibilidad operativa a través de sistemas de supervisión continua y alertas automatizadas facilita la identificación inmediata de caídas. El análisis de logs y el uso de dashboards ayudan a correlacionar eventos y determinar si las interrupciones provienen de fallos de hardware, errores de configuración o mantenimiento no planificado (Tanenbaum y Wetherall, 2014, p. 422).

Registrar los periodos en que cada componente de la infraestructura permanece activo sin degradación de servicio permite calcular indicadores de fiabilidad. Este enfoque granular posibilita identificar dispositivos con alta tasa de fallo y planificar reemplazos o estrategias de redundancia antes de comprometer la disponibilidad global (Harris, 2013, p. 359).

2.2.2.3.2. Porcentaje de disponibilidad del servicio

El porcentaje de uptime se obtiene al dividir el tiempo total operativo entre el periodo evaluado y multiplicarlo por cien. Esta métrica es crítica en la negociación de SLA, ya que especifica el nivel mínimo de servicio esperado y determina penalizaciones por incumplimiento de los niveles acordados (Tanenbaum y Wetherall, 2014, p. 422).

Calcular el uptime combinado con MTBF y MTTR permite a los gestores de red justificar inversiones en tolerancia a fallos. Un porcentaje elevado de disponibilidad refleja la efectividad de estrategias de redundancia, clustering y conmutación por error, esenciales para servicios críticos de la organización (Peltier, 2005, p. 85).

La monitorización de la disponibilidad mediante herramientas SNMP y análisis de tendencias a largo plazo facilita pronósticos de capacidad y mantenimiento preventivo. Conocer la evolución del porcentaje de uptime ayuda a anticipar periodos de presión alta y planificar ventanas de mantenimiento con menor impacto (Harris, 2013, p. 360).

2.2.2.3.3. Tiempo medio de recuperación ante fallas

El MTTR se define como el promedio de tiempo desde la detección de un fallo hasta la plena restauración del servicio. Un MTTR bajo indica procesos de diagnóstico eficientes, procedimientos documentados y personal capacitado para ejecutar

planes de recuperación con rapidez y precisión (Harris, 2013, p. 358).

Realizar simulacros periódicos de recuperación ante desastres permite medir con precisión el MTTR real. Estos ejercicios revelan cuellos de botella en los procedimientos y la infraestructura, posibilitando ajustes en la planificación de recursos y reduciendo el tiempo de inactividad efectivo (Peltier, 2005, p. 142).

Analizar el MTTR junto con el MTBF ayuda a determinar la disponibilidad esperada de la red. Incorporar herramientas de orquestación y automatización en los procesos de recuperación reduce significativamente los tiempos de reparación manual, mejorando la resiliencia operativa (Tanenbaum y Wetherall, 2014, p. 423).

2.2.2.4. Seguridad de red

Según Stallings, (2014), define que

> La seguridad de red en el entorno LAN involucra la implementación de mecanismos de control de acceso, como listas de control de acceso en switches, autenticación en el nivel de puerto y segmentación de red mediante VLAN, junto con el uso de firewalls y sistemas de detección de intrusos capaces de monitorear y bloquear tráfico malicioso antes de que afecte a los usuarios y recursos internos. (p. 312).

Además, Kurose y Ross, (2013), define que

> En una LAN corporativa, la seguridad de red requiere múltiples capas de defensa, incluyendo cifrado de datos en tránsito, autenticación mutua de dispositivos y el uso de protocolos seguros como IPsec. Además, es crucial aplicar actualizaciones de firmware en switches y routers y configurar políticas de seguridad que limiten el acceso a segmentos críticos, reduciendo la superficie de ataque ante amenazas internas y externas (p. 512).

Pfleeger y Pfleeger, (2012), menciona que

> Para garantizar la seguridad de red en un ambiente LAN, es esencial implementar sistemas de prevención de intrusiones (IPS), análisis de logs en tiempo real y segmentar el tráfico en zonas de confianza. Estas prácticas, combinadas con políticas de acceso basadas en roles y la supervisión continua del comportamiento de la red, permiten identificar anomalías y reaccionar rápidamente ante intentos de intrusión (p. 285).

2.2.2.4.1. Número de accesos no autorizados detectados

El recuento de intentos fallidos de acceso a recursos de red proporciona información sobre la eficacia de los controles de autenticación. Un monitoreo sistemático de estos eventos permite identificar patrones de ataque, end points vulnerables y fortalezas o debilidades en las políticas de segmentación (Pfleeger y Pfleeger, 2012, p. 290).

Registrar los accesos no autorizados capturados por sistemas de detección de intrusos (IDS) o SIEM es esencial para evaluar la superficie de ataque. Estos datos, analizados en correlación con la información contextual, ayudan a priorizar parches y ajustes en las reglas de firewall (Tipton y Krause, 2007, p. 334).

El número de accesos bloqueados por controles de puerto y autenticación multifactor refleja la madurez del SGSI. Un aumento en bloqueos exitosos indica que los mecanismos están detectando intentos de intrusión, pero también señala la necesidad de reforzar la visibilidad y la alerta temprana (Whitman y Mattord, 2010, p. 187).

2.2.2.4.2. Presencia de antivirus/firewall activo en la red

La implementación y actualización continua de antivirus en endpoints y servidores es una capa crítica de defensa. Estos sistemas inspeccionan el tráfico en busca de firmas conocidas y

amenazas emergentes, bloqueando actividades maliciosas antes de que comprometan la disponibilidad o la integridad de los datos (Tipton y Krause, 2007, p. 336).

El despliegue de firewalls en el perímetro y en zonas internas de la LAN permite controlar el flujo de paquetes según políticas definidas. Mantener reglas actualizadas y revisar logs periódicamente asegura que solo el tráfico autorizado atraviese los dispositivos de filtrado (Pfleeger y Pfleeger, 2012, p. 292).

La eficiencia de las soluciones de protección perimetral se mide tanto por la tasa de falsas alarmas como por la capacidad de identificar ataques avanzados. La correlación de eventos de antivirus y firewall en un sistema SIEM mejora la visibilidad y reduce los tiempos de respuesta ante incidentes (Stallings, 2014, p. 320).

2.2.2.4.3. Número de incidentes de seguridad reportados

El registro de incidentes de seguridad, desde malware hasta accesos indebidos, sirve para evaluar la madurez del SGSI. Analizar tendencias en la frecuencia y el tipo de incidentes permite priorizar acciones correctivas y mejorar continuamente los controles implementados (Whitman y Mattord, 2010, p. 190).

Un registro detallado de incidentes, complementado con análisis forense digital, facilita la identificación de raíces causales. Esto ayuda a ajustar políticas y procedimientos, reduciendo la probabilidad de recurrencia y fortaleciendo la resiliencia organizacional (Pfleeger y Pfleeger, 2012, p. 295).

El conteo de incidentes reportados por el equipo de soporte técnico refleja tanto la efectividad de los mecanismos de detección como la cultura de reporte interno. Fomentar la comunicación

> transparente sobre fallos mejora la visibilidad de riesgos y refuerza la confianza en el SGSI (Tipton y Krause, 2007, p. 338).

2.3. Bases filosóficas

Sistema de gestión de seguridad de la información

En el estudio de un Sistema de Gestión de Seguridad de la Información (SGSI), las bases filosóficas se despliegan en un entramado coherente que define tanto la naturaleza del objeto de estudio como las prácticas que lo sustentan.

El SGSI considera a la información como un recurso crítico y estructurado, compuesto por flujos de datos y activos —tanto tangibles como intangibles que deben ser protegidos mediante barreras técnicas (cifrado, firewalls) y administrativas (políticas, roles de usuario). Esta concepción asume que la información tiene una existencia objetiva y susceptible de clasificación, valoración y control.

Se adopta un enfoque post-positivista que valida el conocimiento a través de dos vías complementarias: por un lado, mediciones cuantitativas, como los indicadores de confidencialidad, integridad y disponibilidad; por otro, métodos cualitativos entrevistas, análisis de procesos internos y estudio de percepciones de los actores para comprender las dinámicas organizacionales, las brechas de riesgo y la cultura de seguridad.

El SGSI reconoce que cada decisión metodológica y cada política implementada están impregnadas de valores éticos fundamentales: la privacidad de los datos, la responsabilidad de los gestores, la transparencia en los procedimientos, la equidad en el acceso y la confianza mutua entre usuarios y administradores. Estos valores orientan el diseño de controles y la interpretación de resultados, garantizando un compromiso permanente con la protección de derechos y deberes.

El SGSI se sustenta en el ciclo PDCA (Planificar–Hacer–Verificar–Actuar). En la fase de Planificar se definen políticas, objetivos y riesgos; en Hacer, se implementan controles técnicos y formaciones; en Verificar, se ejecutan auditorías, análisis de vulnerabilidades y pruebas de penetración; y en Actuar, se realizan simulacros de recuperación, se ajustan procedimientos y se retroalimenta a los stakeholders. Este proceso iterativo asegura la congruencia entre los supuestos teóricos, los imperativos

normativos y las prácticas operativas, promoviendo la mejora continua y la resiliencia ante amenazas emergentes y cambios regulatorios.

La calidad de servicio de las redes LAN.

En el estudio de la calidad de servicio (QoS) en redes LAN, las bases filosóficas se articulan para definir qué es la QoS, cómo se puede conocer, qué valores la sustentan y qué procedimientos la garantizan.

La QoS en una LAN se concibe como un conjunto de atributos medibles velocidad de transmisión, estabilidad de conexión, disponibilidad, seguridad y satisfacción del usuario que caracterizan la experiencia de comunicación de datos. Ontológicamente, estos atributos existen como propiedades objetivas de la infraestructura (ancho de banda, retardo, pérdida de paquetes) y al mismo tiempo como fenómenos emergentes de la interacción entre componentes físicos, lógicos y humanos.

Para conocer y validar la QoS, el enfoque es híbrido: por un lado, se emplean mediciones cuantitativas throughput, latencia, jitter, MTBF/MTTR recogidas con herramientas de monitoreo; por otro, se recurre al análisis cualitativo de la percepción de los usuarios (encuestas, entrevistas) y de los procesos de gestión de la red. De esta forma se obtiene un conocimiento integral que combina datos duros con la experiencia de quienes utilizan la red.

Los valores que guían el estudio de la QoS son la confiabilidad garantizar el acceso continuo a los recursos, la equidad asegurar que los distintos tipos de tráfico reciban el nivel de servicio pactado, la eficiencia optimizar recursos limitados de manera justa y la usabilidad ofrecer una experiencia satisfactoria al usuario final. Estos valores justifican las elecciones de métricas, la priorización de tráfico y el diseño de políticas de QoS.

2.4. Definición de términos básicos

a) Seguridad confidencial

> “La confidencialidad implica garantizar que la información solo sea accesible a las personas autorizadas, protegiéndola de accesos no autorizados mediante controles técnicos y administrativos” (ISO/IEC, 2018).

b) Seguridad integral

"La seguridad integral considera un enfoque holístico que involucra aspectos técnicos, organizacionales y humanos, con el objetivo de reducir los riesgos que afectan la información" (Venter y Eloff, 2003).

c) Disponibilidad operativa

"La disponibilidad asegura que los usuarios autorizados tengan acceso a la información y a los sistemas asociados cuando lo necesiten, evitando interrupciones en los servicios" (Whitman y Mattord, 2017).

d) Cumplimiento normativo

"El cumplimiento normativo en seguridad de la información implica adherirse a leyes, reglamentos, normas y políticas internas para garantizar una gestión responsable y transparente" (Tipton y Krause, 2007).

e) Velocidad de transmisión

"La velocidad de transmisión o throughput es un parámetro clave que determina cuántos datos pueden ser enviados por segundo a través de una red LAN" (Tanenbaum y Wetherall, 2011).

f) Estabilidad de conexión

"La estabilidad de una conexión en redes LAN está determinada por la baja variabilidad en el retardo de entrega de paquetes, conocida como jitter" (GeeksforGeeks, 2023).

g) Disponibilidad del servicio

"La disponibilidad del servicio en redes LAN se mide por el tiempo en que los recursos están accesibles para los usuarios sin interrupciones significativas" (Kurose y Ross, 2021).

h) Seguridad de red

"La seguridad en redes LAN se logra mediante técnicas como autenticación, cifrado, firewalls y segmentación, que protegen la red frente a accesos no autorizados" (Stallings, 2017).

2.5. Hipótesis de investigación

2.5.1. Hipótesis general

El sistema de gestión de seguridad de la información influye significativamente con la calidad de servicio de las redes LAN en la Municipalidad Distrital de Végueta, Huaura – 2025.

2.5.2. Hipótesis específicas

1. La seguridad confidencial influye significativamente con la calidad de servicio de las redes LAN en la Municipalidad Distrital de Végueta, Huaura – 2025.
2. La seguridad integral influye significativamente con la calidad de servicio de las redes LAN en la Municipalidad Distrital de Végueta, Huaura – 2025.
3. La disponibilidad operativa influye significativamente con la calidad de servicio de las redes LAN en la Municipalidad Distrital de Végueta, Huaura – 2025.
4. El cumplimiento normativo influye significativamente con la calidad de servicio de las redes LAN en la Municipalidad Distrital de Végueta, Huaura – 2025.

2.6. Operacionalización de las variables

VARIABLES	DIMENSIONES	INDICADORES	ESCALA
(X) Sistema de gestión de seguridad de la información	X.1.- Seguridad confidencial	X.1.1.- Acceso restringido a la información X.1.2.- Uso de contraseñas seguras X.1.3.- Control de usuarios y roles	Escala de Likert: Nunca Casi nunca A veces Casi siempre Siempre
	X.2.- Seguridad integral	X.2.1.- Verificación de integridad X.2.2.- Registro de cambios X.2.3.- Prevención de modificaciones no autorizadas	
	X.3.- Disponibilidad operativa	X.3.1.- Tiempo de disponibilidad de los sistemas X.3.2.- Planes de recuperación ante desastres X.3.3.- Mantenimiento periódico de infraestructura	

	X.4.- Cumplimiento normativo	X.4.1.- Adopción de normativas X.4.2.- Auditorías de seguridad de la información X.4.3.- Políticas de seguridad implementadas	
(Y) La calidad de servicio de las redes LAN	Y.1.- Velocidad de transmisión	Y.1.1.- Tasa de transferencia de datos (Mbps) Y.1.2.- Tiempo de respuesta de la red Y.1.3.- Velocidad promedio de carga y descarga	Escala de Likert: Nunca Casi nunca A veces Casi siempre Siempre
	Y.2.- Estabilidad de conexión	Y.2.1.- Frecuencia de caídas de red por semana Y.2.2.- Fluctuación del ancho de banda Y.2.3.- Variación en el tiempo de respuesta	
	Y.3.- Disponibilidad del servicio	Y.3.1.- Tiempo total de red operativa Y.3.2.- Porcentaje de disponibilidad del servicio Y.3.3.- Tiempo medio de recuperación ante fallas	
	Y.4.- Seguridad de red	Y.4.1.- Número de accesos no autorizados detectados Y.4.2.- Presencia de antivirus/firewall activo en la red Y.4.3.- Número de incidentes de seguridad reportados	

CAPÍTULO III. METODOLOGÍA

3.1. Diseño metodológico

3.1.1. Tipo de Investigación

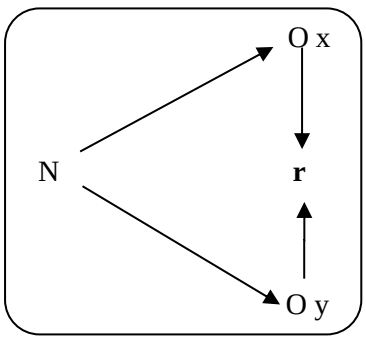
El tipo de investigación es aplicado, ya que busca generar conocimientos con un propósito práctico, orientado a la solución de problemas específicos dentro del contexto de estudio. (Hernández, Fernández y Baptista, 2014).

3.1.2. Nivel

El nivel de investigación es correlacional, puesto que tiene como objetivo analizar la relación entre dos o más variables sin manipularlas, permitiendo establecer el grado de asociación entre ellas a partir de la recolección de datos en un entorno real. (Hernández, Fernández y Baptista, 2014).

3.1.3. Diseño

El diseño de la investigación no es experimental y de corte transversal. Según Hernández, Fernández y Baptista (2014), un estudio no experimental se caracteriza por la observación y análisis de los fenómenos tal como se presentan en su contexto natural, sin intervención directa del investigador sobre las variables. Además, el diseño transversal implica que los datos serán recolectados en un solo momento en el tiempo, lo que permite identificar y examinar relaciones entre las variables sin realizar un seguimiento a lo largo del tiempo. Cómo podemos ver en la siguiente figura:



Denotación:

N = Población

Ox = Observación a la variable independiente.

Oy = Observación a la variable dependiente.

r = Relación entre variables.

3.1.4 Enfoque

El enfoque de la investigación es cuantitativo, ya que se fundamenta en la recopilación y análisis de datos numéricos para probar hipótesis y establecer patrones de relación entre variables (Creswell, 2014). Para ello, se aplicarán encuestas que permitirán obtener información precisa y objetiva.

3.2. Población y muestra

3.2.1. Población

Córdoba (2009) señalo que: "La población es el conjunto bien definido de unidades de observación con características comunes y perceptibles. Es denotado por la letra N".

El universo poblacional estuvo constituido por 52 trabajadores de la Municipalidad Distrital de Végueta, Huaura - 2025.

3.2.2. Muestra

El universo poblacional estuvo constituido por 52 trabajadores de la Municipalidad Distrital de Végueta, Huaura - 2025.

Por ser pequeña la población se consideró una muestra no probabilística, porque el investigador, conociendo bien la población y con el buen criterio, decide que las unidades de observación integrarán la muestra. Se hará uso del método, o técnica de muestreo llamado muestreo intencional u opinático, con el criterio de conveniencia del investigador para que sean representativas, la muestra se aplicó a la totalidad de los elementos de observación con las mismas características, según Córdoba (2009 pg. 32) en su libro denominado Estadística aplicada a la Investigación.

3.3. Técnicas de recolección de datos

Las técnicas e instrumentos que se utilizo en el presente trabajo de investigación se muestran a continuación:

Técnicas:

- Encuesta

García (1993) define como:

Una técnica que utiliza un conjunto de procedimientos estandarizados de investigación mediante los cuales se recoge y analiza una serie de datos de una muestra de casos representativa de una población o universo más amplio, del que se pretende explorar, describir, predecir y/o explicar una serie de características.

Instrumentos:

- Cuestionario de preguntas.

García (1993) define como: "Documento que recoge de forma organizada los indicadores de las variables implicadas en el objetivo de la encuesta."

3.4. Técnicas para el procedimiento de la información

A través de la entrevista y su instrumento – cuestionario, elaborado por el tesista especialmente para esta investigación, se recopilo información sobre cada una de las dimensiones de la variable, las preguntas estarán referidas a los aspectos concretos que aportarán para recopilar datos y ubicar las deficiencias en la Vd.

Mediante la observación y su respectivo instrumento vamos a comprender procesos, interrelaciones entre personas y sus situaciones o circunstancias y eventos que suceden a través del tiempo, así como los patrones que se desarrollan y los contextos sociales y culturales en los cuales ocurren las experiencias humanas; así como identificar problemas.

a) Ficha técnica de instrumentos

La encuesta estuvo constituida por preguntas de la Vi y la Vd., la medición se hará a través de la Escala de Likert, que mide de 1 a 5.

b) Administración de los instrumentos y obtención de los datos

Para el acopio de la información se formuló y conto con un cuestionario, confiable y validado por especialistas y expertos en la investigación, que darán su opinión de expertos si el cuestionario es aplicable o puede ser observado para luego ser corregido por el investigador. La confiabilidad se logrará aplicando pruebas pilotos que fueron aplicados el cuestionario varias veces a la muestra determinada para comprobar la precisión y exactitud del instrumento o en todo caso hacemos uso de la prueba de Alfa de Cronbach.

En la administración de cuestionarios se contó con el valioso apoyo en la recopilación de datos del personal.

Análisis Estadístico

Se llevo a cabo utilizando el paquete estadístico SPSS 25.0 el cual procesará, para lograr la interpretación, análisis y discusión los gráficos y figuras estadísticos, para lograr los resultados y contar con las conclusiones, implicando los objetivos y las hipótesis que fue el producto final de la investigación.

Formulación del modelo

a. Hipótesis Nula.

Existen evidencias que las medias de los tratamientos estadísticamente no difieren significativamente.

b. Hipótesis alterna.

Estadísticamente las medias de los tratamientos difieren significativamente.

c. Recolección de datos y cálculos de los estadísticos correspondientes.

La recolección de datos se efectuó una vez aplicado los tratamientos correspondientes a cada muestra y para el procesamiento se utilizó programas estadísticos.

d. Decisión estadística.

La decisión estadística se tomó como consecuencia de la comparación del estadístico de prueba calculado y el obtenido mediante tablas estadísticas correspondientes a la distribución del estadístico de prueba; esto quiere decir si el

valor del estadístico de prueba calculado se encuentra en la región de rechazo se rechaza la hipótesis nula, en caso contrario se acepta; es decir:

Si: **$F0 > F\alpha, a-1, N-a$ se rechaza**

CAPÍTULO IV. RESULTADOS

4.1. Análisis de resultados

Tabla 1

Sistema de gestión de seguridad de la información

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	4	7,7	7,7	7,7
	Casi Nunca	16	30,8	30,8	38,5
	A Veces	22	42,3	42,3	80,8
	Casi Siempre	7	13,5	13,5	94,2
	Siempre	3	5,8	5,8	100,0
	Total	52	100,0	100,0	

Para efectos de mejor apreciación y comparación se presenta la siguiente figura:

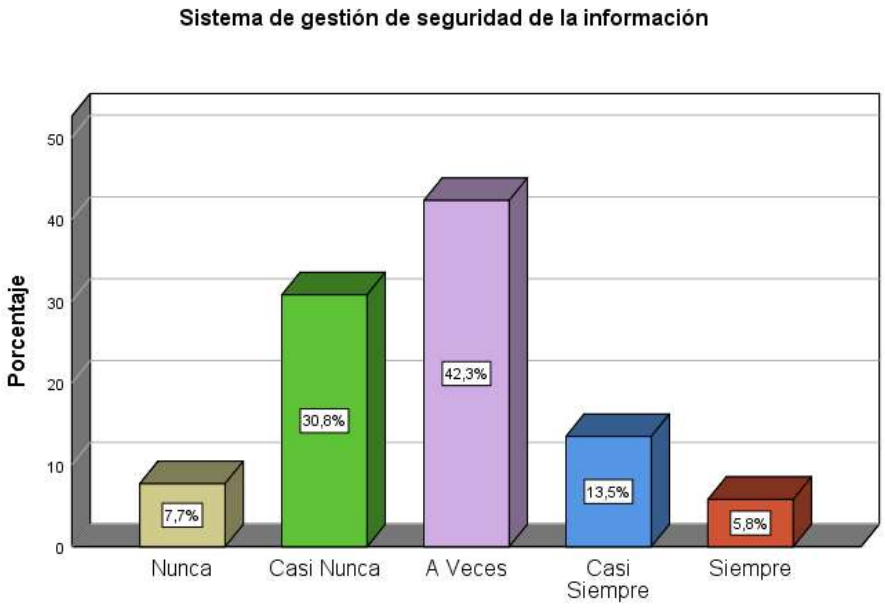


Figura 2. Sistema de gestión de seguridad de la información

De la figura 2, un 42,3% (22) de los trabajadores de la Municipalidad Distrital de Végueta, Huaura manifestó que a veces se aplica el sistema de gestión de seguridad de la información, siendo este el grupo más representativo. Le sigue un 30,8% (16) que indicó que casi nunca se implementa dicho sistema, mientras que un 13,5% (7) señaló que casi siempre se aplica. Finalmente, un 7,7% (4) expresó que nunca se utiliza y solo un 5,8% (3) afirmó que siempre se aplica en la institución.

Tabla 2

Seguridad confidencial

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	3	5,8	5,8	5,8
	Casi Nunca	16	30,8	30,8	36,5
	A Veces	25	48,1	48,1	84,6
	Casi Siempre	5	9,6	9,6	94,2
	Siempre	3	5,8	5,8	100,0
	Total	52	100,0	100,0	

Para efectos de mejor apreciación y comparación se presenta la siguiente figura:

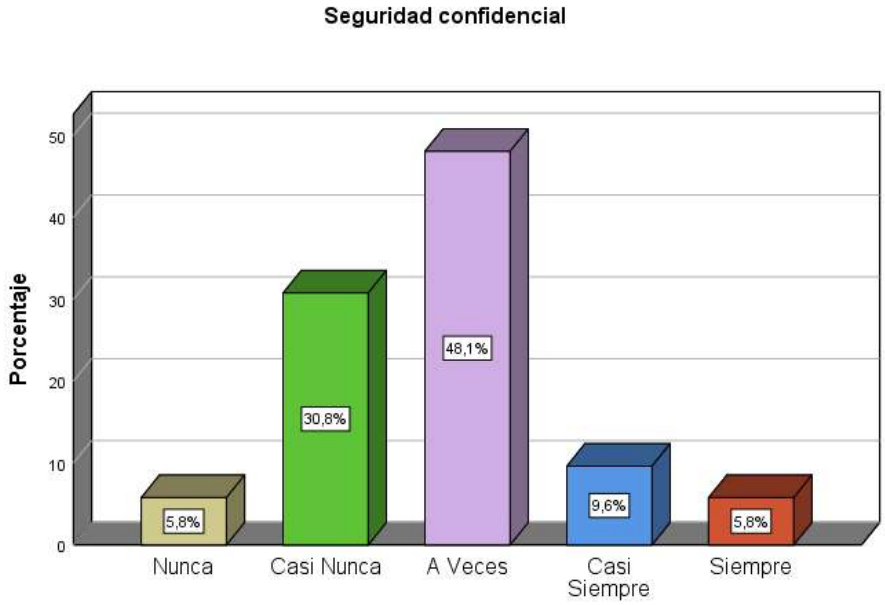


Figura 3. Seguridad confidencial

De la figura 3, un 48,1% (25) de los trabajadores de la Municipalidad Distrital de Végueta, Huaura manifestó que a veces se mantiene la seguridad confidencial, siendo este el grupo más representativo. Le sigue un 30,8% (16) que indicó que casi nunca se garantiza dicha seguridad, mientras que un 9,6% (5) señaló que casi siempre se cumple con este aspecto. Finalmente, un 5,8% (3) expresó que nunca se mantiene y otro 5,8% (3) afirmó que siempre se preserva la seguridad confidencial en la institución.

Tabla 3

Seguridad integral

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	7	13,5	13,5	13,5
	Casi Nunca	13	25,0	25,0	38,5
	A Veces	12	23,1	23,1	61,5
	Casi Siempre	9	17,3	17,3	78,8
	Siempre	11	21,2	21,2	100,0
	Total	52	100,0	100,0	

Para efectos de mejor apreciación y comparación se presenta la siguiente figura:

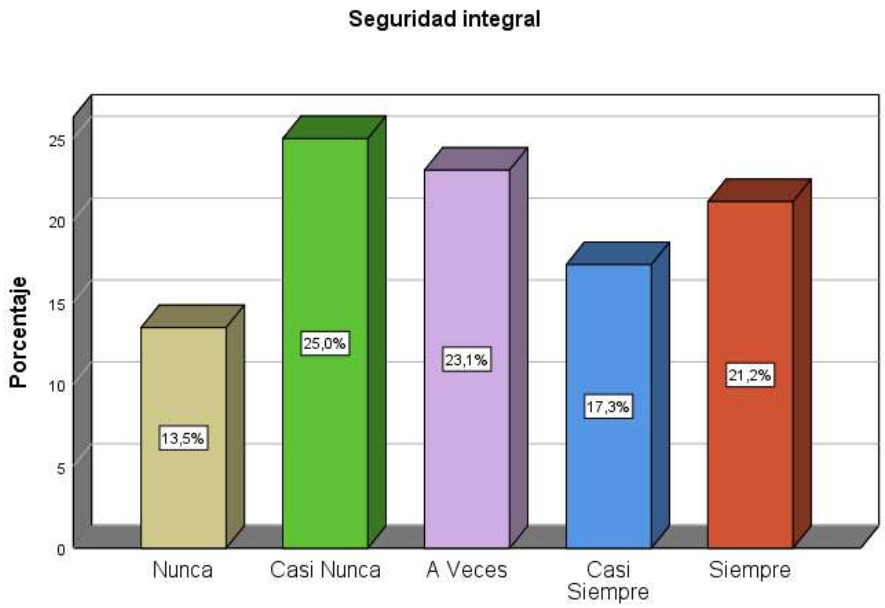


Figura 4. Seguridad integral

De la figura 4, un 25,0% (13) de los trabajadores de la Municipalidad Distrital de Végueta, Huaura manifestó que casi nunca se aplica la seguridad integral, siendo este el grupo más representativo. Le sigue un 23,1% (12) que indicó que a veces se cumple con este aspecto, mientras que un 21,2% (11) señaló que siempre se aplica. Por otro lado, un 17,3% (9) expresó que casi siempre se implementa y un 13,5% (7) afirmó que nunca se aplica la seguridad integral en la institución.

Tabla 4

Disponibilidad operativa

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	7	13,5	13,5	13,5
	Casi Nunca	18	34,6	34,6	48,1
	A Veces	11	21,2	21,2	69,2
	Casi Siempre	6	11,5	11,5	80,8
	Siempre	10	19,2	19,2	100,0
	Total	52	100,0	100,0	

Para efectos de mejor apreciación y comparación se presenta la siguiente figura:

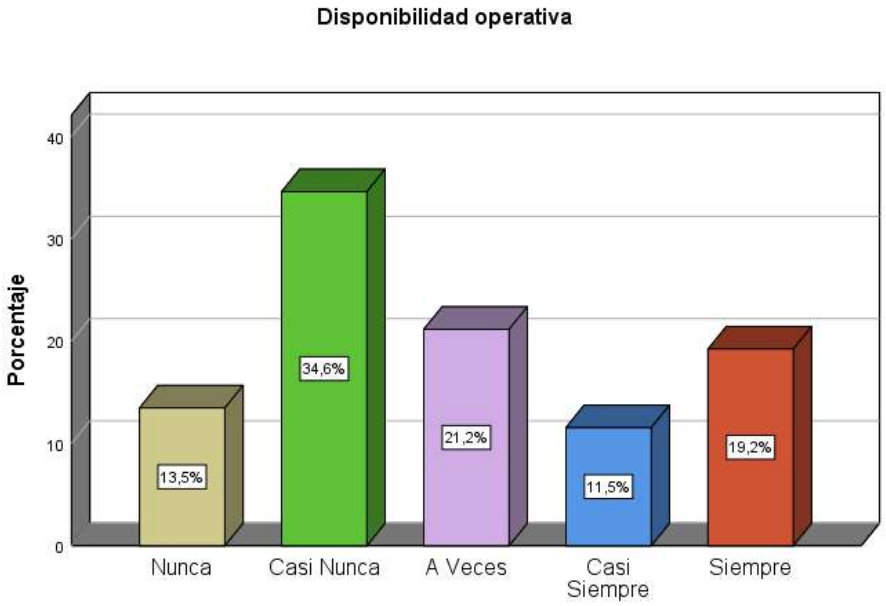


Figura 5. Disponibilidad operativa

De la figura 5, un 34,6% (18) de los trabajadores de la Municipalidad Distrital de Végueta, Huaura manifestó que casi nunca se mantiene la disponibilidad operativa, siendo este el grupo más representativo. Le sigue un 21,2% (11) que indicó que a veces se garantiza este aspecto, mientras que un 19,2% (10) señaló que siempre se cumple. Por otro lado, un 13,5% (7) expresó que nunca se mantiene y un 11,5% (6) afirmó que casi siempre se asegura la disponibilidad operativa en la institución.

Tabla 5

Cumplimiento normativo

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	7	13,5	13,5	13,5
	Casi Nunca	23	44,2	44,2	57,7
	A Veces	10	19,2	19,2	76,9
	Casi Siempre	2	3,8	3,8	80,8
	Siempre	10	19,2	19,2	100,0
	Total	52	100,0	100,0	

Para efectos de mejor apreciación y comparación se presenta la siguiente figura:

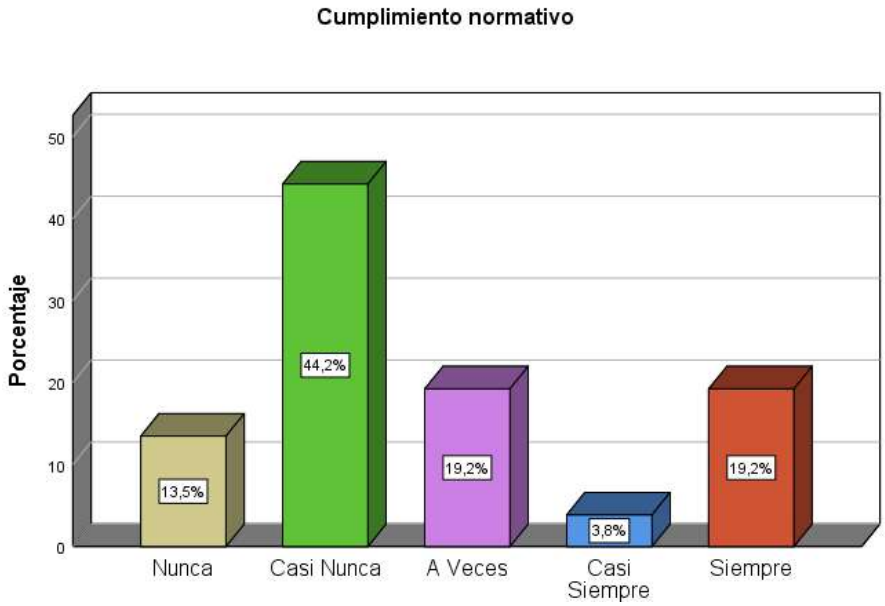


Figura 6. Cumplimiento normativo

De la figura 6, un 44,2% (23) de los trabajadores de la Municipalidad Distrital de Végueta, Huaura manifestó que casi nunca se cumple con las normas establecidas, siendo este el grupo más representativo. Le sigue un 19,2% (10) que indicó que a veces se respeta el cumplimiento normativo, mientras que otro 19,2% (10) señaló que siempre se acata. Por otro lado, un 13,5% (7) expresó que nunca se cumple y un 3,8% (2) afirmó que casi siempre se respetan las normas dentro de la institución.

Tabla 6

La calidad de servicio de las redes LAN

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	5	9,6	9,6	9,6
	Casi Nunca	24	46,2	46,2	55,8
	A Veces	14	26,9	26,9	82,7
	Casi Siempre	4	7,7	7,7	90,4
	Siempre	5	9,6	9,6	100,0
	Total	52	100,0	100,0	

Para efectos de mejor apreciación y comparación se presenta la siguiente figura:

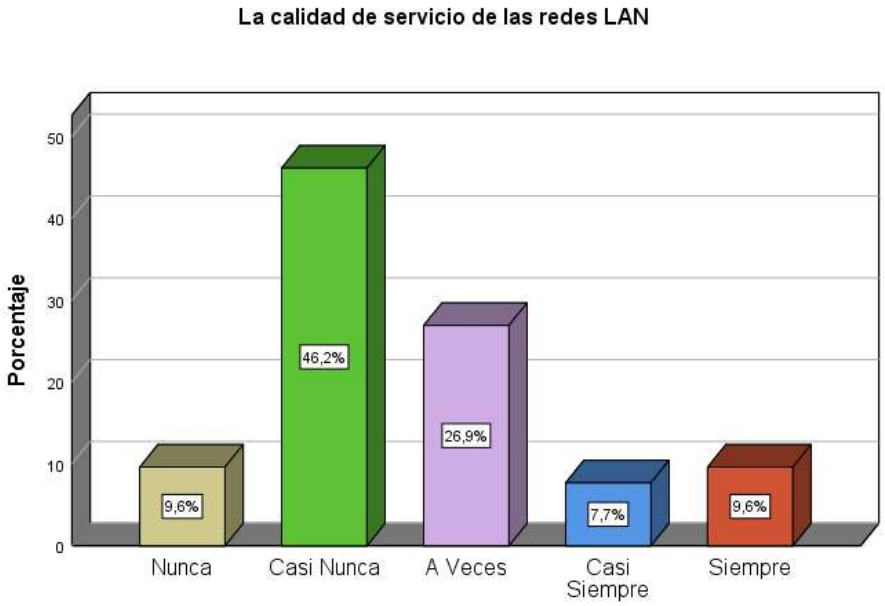


Figura 7. La calidad de servicio de las redes LAN

De la figura 7, un 46,2% (24) de los trabajadores de la Municipalidad Distrital de Végueta, Huaura manifestó que casi nunca se garantiza la calidad del servicio de las redes LAN, siendo este el grupo más representativo. Le sigue un 26,9% (14) que indicó que a veces se mantiene un servicio adecuado, mientras que un 9,6% (5) señaló que siempre se cumple con la calidad esperada. Por otro lado, un 9,6% (5) expresó que nunca se asegura y un 7,7% (4) afirmó que casi siempre se garantiza la calidad del servicio de las redes LAN en la institución.

Tabla 7

Velocidad de transmisión

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	5	9,6	9,6	9,6
	Casi Nunca	22	42,3	42,3	51,9
	A Veces	13	25,0	25,0	76,9
	Casi Siempre	4	7,7	7,7	84,6
	Siempre	8	15,4	15,4	100,0
	Total	52	100,0	100,0	

Para efectos de mejor apreciación y comparación se presenta la siguiente figura:

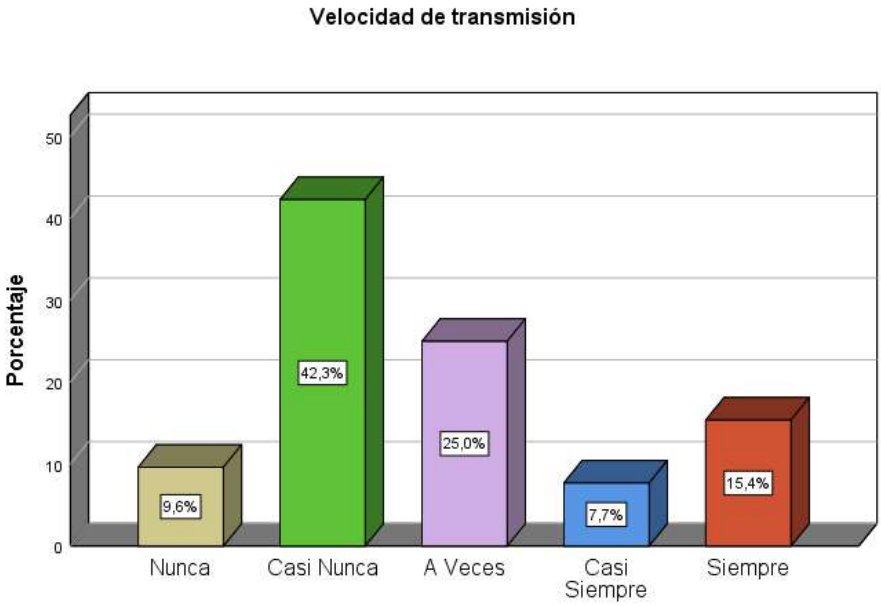


Figura 8. Velocidad de transmisión

De la figura 8, un 42,3% (22) de los trabajadores de la Municipalidad Distrital de Végueta, Huaura manifestó que casi nunca se mantiene una adecuada velocidad de transmisión, siendo este el grupo más representativo. Le sigue un 25,0% (13) que indicó que a veces se garantiza este aspecto, mientras que un 15,4% (8) señaló que siempre se cumple con una transmisión eficiente. Por otro lado, un 9,6% (5) expresó que nunca se mantiene y un 7,7% (4) afirmó que casi siempre se logra una buena velocidad de transmisión en la institución.

Tabla 8

Estabilidad de conexión

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	5	9,6	9,6	9,6
	Casi Nunca	18	34,6	34,6	44,2
	A Veces	17	32,7	32,7	76,9
	Casi Siempre	5	9,6	9,6	86,5
	Siempre	7	13,5	13,5	100,0
	Total	52	100,0	100,0	

Para efectos de mejor apreciación y comparación se presenta la siguiente figura:

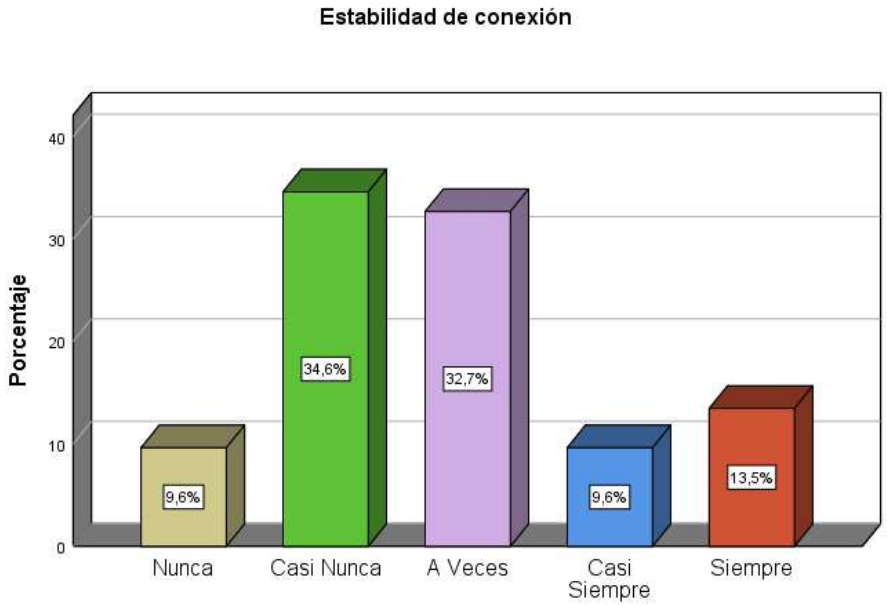


Figura 9. Estabilidad de conexión

De la figura 9, un 34,6% (18) de los trabajadores de la Municipalidad Distrital de Végueta, Huaura manifestó que casi nunca se mantiene la estabilidad de conexión, siendo este el grupo más representativo. Le sigue un 32,7% (17) que indicó que a veces se garantiza este aspecto, mientras que un 13,5% (7) señaló que siempre se mantiene una conexión estable. Por otro lado, un 9,6% (5) expresó que nunca se asegura y otro 9,6% (5) afirmó que casi siempre se logra la estabilidad de conexión en la institución.

Tabla 9

Disponibilidad del servicio

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	2	3,8	3,8	3,8
	Casi Nunca	23	44,2	44,2	48,1
	A Veces	17	32,7	32,7	80,8
	Casi Siempre	2	3,8	3,8	84,6
	Siempre	8	15,4	15,4	100,0
	Total	52	100,0	100,0	

Para efectos de mejor apreciación y comparación se presenta la siguiente figura:

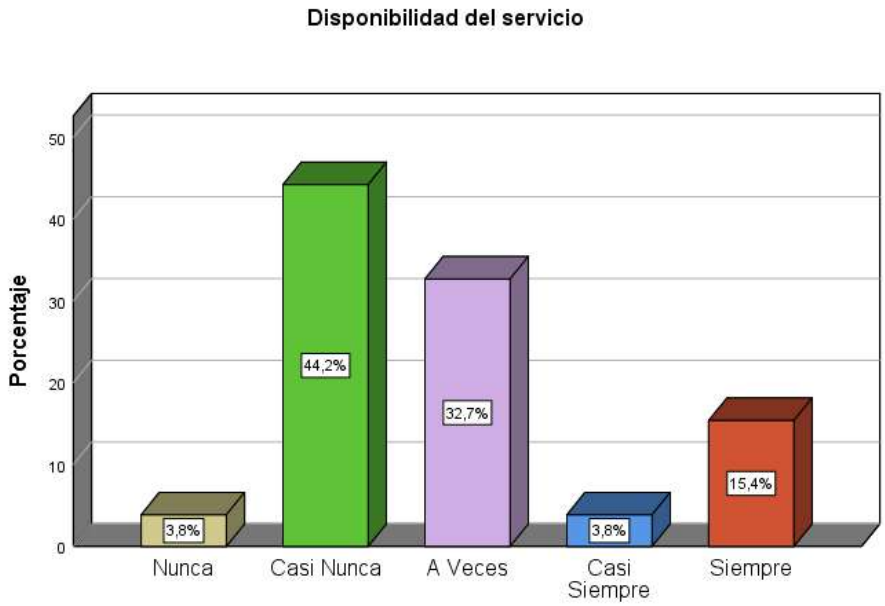


Figura 10. Disponibilidad del servicio

De la figura 10, un 44,2% (23) de los trabajadores de la Municipalidad Distrital de Végueta, Huaura manifestó que casi nunca se garantiza la disponibilidad del servicio, siendo este el grupo más representativo. Le sigue un 32,7% (17) que indicó que a veces se mantiene este aspecto, mientras que un 15,4% (8) señaló que siempre se cumple con la disponibilidad. Por otro lado, un 3,8% (2) expresó que nunca se asegura y otro 3,8% (2) afirmó que casi siempre se garantiza la disponibilidad del servicio en la institución.

Tabla 10

Seguridad de red

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	5	9,6	9,6	9,6
	Casi Nunca	21	40,4	40,4	50,0
	A Veces	14	26,9	26,9	76,9
	Casi Siempre	4	7,7	7,7	84,6
	Siempre	8	15,4	15,4	100,0
	Total	52	100,0	100,0	

Para efectos de mejor apreciación y comparación se presenta la siguiente figura:

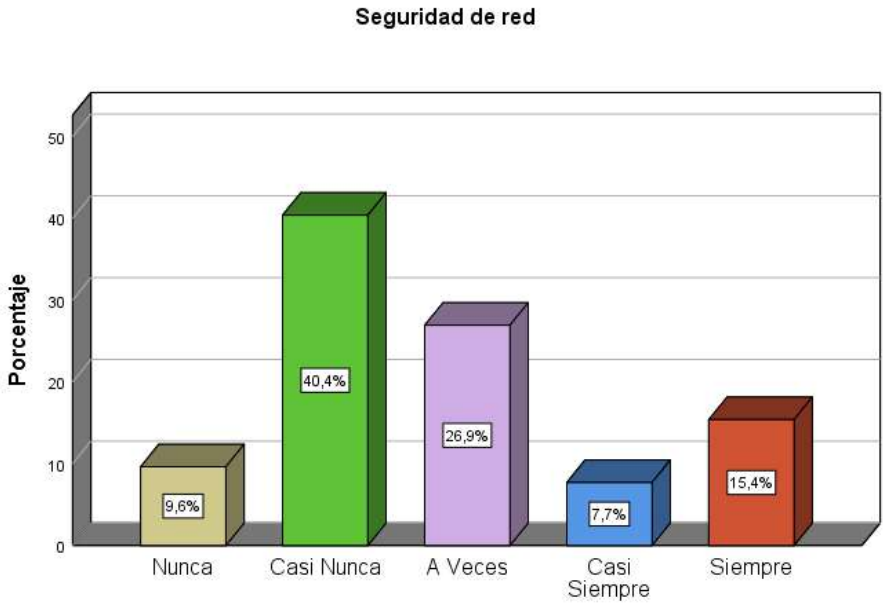


Figura 11. Seguridad de red

De la figura 11, un 40,4% (21) de los trabajadores de la Municipalidad Distrital de Végueta, Huaura manifestó que casi nunca se garantiza la seguridad de red, siendo este el grupo más representativo. Le sigue un 26,9% (14) que indicó que a veces se mantiene este aspecto, mientras que un 15,4% (8) señaló que siempre se cumple con la seguridad. Por otro lado, un 9,6% (5) expresó que nunca se asegura y un 7,7% (4) afirmó que casi siempre se garantiza la seguridad de red en la institución.

4.2. Contrastación de hipótesis

Dado que se tiene 2 variables cuantitativas es necesario comprobar antes de cualquier análisis estadístico inferencial, si los datos de las variables aleatorias estudiadas siguen o no el modelo normal de distribución de probabilidades. Para realizar la prueba de normalidad se utilizó la prueba de Kolmogórov-Smirnov, dado que el tamaño de la muestra es mayor que 50.

Prueba de Normalidad de las variables sistema de gestión de seguridad de la información y la calidad de servicio de las redes LAN

Para realizar la prueba de normalidad de las variables sistema de gestión de seguridad de la información y la calidad de servicio de las redes LAN se utilizó la prueba de Kolmogórov-Smirnov y se siguió el siguiente procedimiento:

a) Planteo de las hipótesis:

   Hipótesis Nula (H_0): Las puntuaciones de las variables sistema de gestión de seguridad de la información y la calidad de servicio de las redes LAN tienen una distribución normal

   Hipótesis Alterna (H_a): Las puntuaciones de la variable sistema de gestión de seguridad de la información y la calidad de servicio de las redes LAN no tienen una distribución normal**.**

b) Nivel de significación o riesgo: $\alpha = 5\% = 0{,}05$

c) Estadístico de prueba: Kolmogórov-Smirnov

Tabla 11

Prueba de normalidad de las variables sistema de gestión de seguridad de la información y la calidad de servicio de las redes LAN

	Kolmogórov-Smirnov		
	Estadístico	gl	Sig.
Sistema de gestión de seguridad de la información	,101	52	,000
La calidad de servicio de las redes LAN	,145	52	,000

a. Corrección de significación de Lilliefors

d) Regla de decisión:

- Si: P_valor (Sig) ≤ 0,05 se rechaza la hipótesis nula
- Si: P_valor (Sig) > 0,05 no se rechaza la hipótesis nula

Sobre las variables sistema de gestión de seguridad de la información y la calidad de servicio de las redes LAN, el p-valor=Sig= es igual ,000 como este valor es menos a 0,05 se infiere que hay suficiente evidencia estadística para rechazar la hipótesis nula, concluyendo que los datos no provienen de una distribución normal.

Hipótesis General

Hipótesis Alternativa: El sistema de gestión de seguridad de la información influye significativamente con la calidad de servicio de las redes LAN en la Municipalidad Distrital de Végueta, Huaura – 2025.

Hipótesis nula: El sistema de gestión de seguridad de la información no influye significativamente con la calidad de servicio de las redes LAN en la Municipalidad Distrital de Végueta, Huaura – 2025.

Tabla 12

El sistema de gestión de seguridad de la información y la calidad de servicio de las redes LAN

			Sistema de gestión de seguridad de la información	La calidad de servicio de las redes LAN
Rho de Spearman	Sistema de gestión de seguridad de la información	Coeficiente de correlación	1,000	,736**
		Sig. (bilateral)	.	,000
		N	52	52
	La calidad de servicio de las redes LAN	Coeficiente de correlación	,736**	1,000
		Sig. (bilateral)	,000	.
		N	52	52

**. La correlación es significativa en el nivel 0,01 (bilateral).

Como se muestra en la tabla 12 se obtuvo un coeficiente de correlación de r= 0.736, con una p=0.000(p<0.05) con lo cual se acepta la hipótesis alternativa y se rechaza la hipótesis nula. Por lo tanto, se puede evidenciar estadísticamente que el sistema de gestión de seguridad de la información influye significativamente con la calidad de servicio de las redes LAN en la Municipalidad Distrital de Végueta, Huaura – 2025.

Se puede apreciar que el coeficiente de correlación es de una magnitud de correlación positiva alta.

Hipótesis Especifica 1

Hipótesis Alternativa: La seguridad confidencial influye significativamente con la calidad de servicio de las redes LAN en la Municipalidad Distrital de Végueta, Huaura – 2025.

Hipótesis nula: La seguridad confidencial no influye significativamente con la calidad de servicio de las redes LAN en la Municipalidad Distrital de Végueta, Huaura – 2025.

Tabla 13

La seguridad confidencial y la calidad de servicio de las redes LAN

			Seguridad confidencial	La calidad de servicio de las redes LAN
Rho de Spearman	Seguridad confidencial	Coeficiente de correlación	1,000	,615**
		Sig. (bilateral)	.	,000
		N	52	52
	La calidad de servicio de las redes LAN	Coeficiente de correlación	,615**	1,000
		Sig. (bilateral)	,000	.
		N	52	52

**. La correlación es significativa en el nivel 0,01 (bilateral).

Como se muestra en la tabla 13 se obtuvo un coeficiente de correlación de r= 0.615, con una p=0.000(p<0.05) con lo cual se acepta la hipótesis alternativa y se rechaza la hipótesis nula. Por lo tanto, se puede evidenciar estadísticamente que la seguridad confidencial influye significativamente con la calidad de servicio de las redes LAN en la Municipalidad Distrital de Végueta, Huaura – 2025.

Se puede apreciar que el coeficiente de correlación es de una magnitud de correlación positiva alta.

Hipótesis Especifica 2

Hipótesis Alternativa: La seguridad integral influye significativamente con la calidad de servicio de las redes LAN en la Municipalidad Distrital de Végueta, Huaura – 2025.

Hipótesis nula: La seguridad integral no influye significativamente con la calidad de servicio de las redes LAN en la Municipalidad Distrital de Végueta, Huaura – 2025.

Tabla 14

La seguridad integral y la calidad de servicio de las redes LAN

			Seguridad integral	La calidad de servicio de las redes LAN
Rho de Spearman	Seguridad integral	Coeficiente de correlación	1,000	,623**
		Sig. (bilateral)	.	,000
		N	52	52
	La calidad de servicio de las redes LAN	Coeficiente de correlación	,623**	1,000
		Sig. (bilateral)	,000	.
		N	52	52

**. La correlación es significativa en el nivel 0,01 (bilateral).

Como se muestra en la tabla 14 se obtuvo un coeficiente de correlación de r= 0.623, con una p=0.000(p<0.05) con lo cual se acepta la hipótesis alternativa y se rechaza la hipótesis nula. Por lo tanto, se puede evidenciar estadísticamente que la seguridad integral influye significativamente con la calidad de servicio de las redes LAN en la Municipalidad Distrital de Végueta, Huaura – 2025.

Se puede apreciar que el coeficiente de correlación es de una magnitud de correlación positiva alta.

Hipótesis Especifica 3

Hipótesis Alternativa: La disponibilidad operativa influye significativamente con la calidad de servicio de las redes LAN en la Municipalidad Distrital de Végueta, Huaura – 2025.

Hipótesis nula: La disponibilidad operativa no influye significativamente con la calidad de servicio de las redes LAN en la Municipalidad Distrital de Végueta, Huaura – 2025.

Tabla 15

La disponibilidad operativa y la calidad de servicio de las redes LAN

			Disponibilidad operativa	La calidad de servicio de las redes LAN
Rho de Spearman	Disponibilidad operativa	Coeficiente de correlación	1,000	,751**
		Sig. (bilateral)	.	,000
		N	52	52
	La calidad de servicio de las redes LAN	Coeficiente de correlación	,751**	1,000
		Sig. (bilateral)	,000	.
		N	52	52

**. La correlación es significativa en el nivel 0,01 (bilateral).

Como se muestra en la tabla 15 se obtuvo un coeficiente de correlación de r= 0.751, con una p=0.000(p<0.05) con lo cual se acepta la hipótesis alternativa y se rechaza la hipótesis nula. Por lo tanto, se puede evidenciar estadísticamente que la disponibilidad operativa influye significativamente con la calidad de servicio de las redes LAN en la Municipalidad Distrital de Végueta, Huaura – 2025.

Se puede apreciar que el coeficiente de correlación es de una magnitud de correlación positiva alta.

Hipótesis Especifica 4

Hipótesis Alternativa: El cumplimiento normativo influye significativamente con la calidad de servicio de las redes LAN en la Municipalidad Distrital de Végueta, Huaura – 2025.

Hipótesis nula: El cumplimiento normativo no influye significativamente con la calidad de servicio de las redes LAN en la Municipalidad Distrital de Végueta, Huaura – 2025.

Tabla 16

El cumplimiento normativo y la calidad de servicio de las redes LAN

			Cumplimiento normativo	La calidad de servicio de las redes LAN
Rho de Spearman	Cumplimiento normativo	Coeficiente de correlación	1,000	,771**
		Sig. (bilateral)	.	,000
		N	52	52
	La calidad de servicio de las redes LAN	Coeficiente de correlación	,771**	1,000
		Sig. (bilateral)	,000	.
		N	52	52

**. La correlación es significativa en el nivel 0,01 (bilateral).

Como se muestra en la tabla 16 se obtuvo un coeficiente de correlación de r= 0.771, con una p=0.000(p<0.05) con lo cual se acepta la hipótesis alternativa y se rechaza la hipótesis nula. Por lo tanto, se puede evidenciar estadísticamente que el cumplimiento normativo influye significativamente con la calidad de servicio de las redes LAN en la Municipalidad Distrital de Végueta, Huaura – 2025.

Se puede apreciar que el coeficiente de correlación es de una magnitud de correlación positiva alta.

CAPÍTULO V. DISCUSIÓN

5.1. Discusión de resultados

Los resultados estadísticos indican que el sistema de gestión de seguridad de la información influye significativamente con la calidad de servicio de las redes LAN en la Municipalidad Distrital de Végueta, Huaura – 2025, evidenciado por una correlación de Spearman de 0.736, lo cual representa una magnitud de correlación positiva alta. Este hallazgo guarda similitudes con el estudio de Galindo (2022) quien evidencio que para el contraste de correlación de Pearson se determinó que el valor hallado del coeficiente de correlación fue r = 0,540 (valor de p = 0,000); por lo tanto, existe una influencia directa y significativa entre el SGSI y la Calidad de Servicio de la Red LAN de la Municipalidad Distrital de Ilabaya. Quiere decir que existe una relación directa y significativa entre el SGSI y la Calidad de Servicio de las redes LAN en la Municipalidad Distrital de Ilabaya, es evidencia necesaria para el inicio de la implementación de un SGSI, lo cual se planteó al área encargada el diseño de SGSI iniciando con un análisis situacional de la entidad posteriormente se desarrolló políticas y controles de seguridad para la Municipalidad distrital de Ilabaya.

Al analizar las dimensiones específicas de las variables, se observa que la seguridad confidencial influye significativamente con la calidad de servicio de las redes LAN en la Municipalidad Distrital de Végueta, Huaura – 2025. Esto se refleja en una correlación de Spearman de 0.615, lo que indica correlación positiva alta. Este hallazgo se alinea con el estudio de Suazo (2024), indicaron que el modelo de correlación de Rho de Spearman devuelve un coeficiente de 0,142 y una significancia de 0,020 por lo que se puede comprobar, con un 95% de probabilidad, que existe una correlación positiva baja entre el sistema de gestión de seguridad de la información y la calidad de servicio de las redes en la empresa Cerámica Lima S.A. en el 2023.

De acuerdo en la segunda dimensión, se observa que la seguridad integral influye significativamente con la calidad de servicio de las redes LAN en la Municipalidad Distrital de Végueta, Huaura – 2025. Esto se refleja en una correlación de Spearman de 0.623, lo que indica correlación positiva alta. Este hallazgo se alinea con el estudio de Martínez (2023) indicaron que se verifico que, si existe una coherencia entre las

variables de SGSI y la calidad del servicio, accediendo a plantear los problemas de seguridad en la información, todo esto para mejorar sus procesos de la mano con la normativa ISO 27001, lo cual mejorará en minimizar la perdida de información. Así mismo se observó que el personal tenía poco conocimiento en cuanto ciberseguridad. Además, al identificar los principios de S.I. en correlación a la calidad del servicio del colegio Carlos A. Velásquez Ilo fue implantar orientaciones en la S.I de los sistemas que maneja el colegio.

También en la tercera dimensión, se observa que la disponibilidad operativa influye significativamente con la calidad de servicio de las redes LAN en la Municipalidad Distrital de Végueta, Huaura – 2025. Esto se refleja en una correlación de Spearman de 0.751, lo que indica correlación positiva alta. Este hallazgo se alinea con el estudio de Calcina (2023) indicaron que que se diseñó e implementó una nueva red, luego, se comprobó la mejora de la calidad de servicio a través del diseño, implementación e integración de una nueva red LAN con tecnología CISCO en la Unidad Minera San Rafael, para ello se utilizó la prueba de diferencias de medias, donde se obtuvo que los tiempos de respuesta y latencias con la nueva red LAN son significativamente menores a la red anterior (en el nivel de significancia del 0.05).

Finalmente, en la cuarta dimensión, se observa que el cumplimiento normativo influye significativamente con la calidad de servicio de las redes LAN en la Municipalidad Distrital de Végueta, Huaura – 2025. Esto se refleja en una correlación de Spearman de 0.771, lo que indica correlación positiva alta. Este hallazgo encuentra resonancia en la investigación de Avalos (2020) quien evidenció que, que la administración es mucho más sencilla y fácil de manejar, siendo lo más importante, la correcta gestión de las asignaciones de las ips, lo cual nos permite ahorrar tiempo en el diagnóstico y anticiparnos a cualquier inconveniente. El proyecto ha ayudado a diagnosticar con mayor rapidez y tener un mayor control de los servicios, lo cual lo hemos visto reflejado en la disminución del tiempo de atención en la base de datos semanal. El tener una arquitectura redundante en diferentes data centers, nos permite tener el respaldo que necesitamos ante cualquier problema físico ya ocurrido.

CAPÍTULO VI. CONCLUSIONES Y RECOMENDACIONES

6.1. Conclusiones

De las pruebas realizadas podemos concluir:

1. **Según el objetivo general**, esta tesis logró evidenciar que el sistema de gestión de seguridad de la información influye significativamente con la calidad de servicio de las redes LAN en la Municipalidad Distrital de Végueta, Huaura – 2025, debido a la clasificación de Pearson que devuelve un valor de 0,736, lo que indica una correlación positiva alta. Porque un mejor sistema de seguridad permite que las redes funcionen de forma más estable, confiable y eficiente.
2. **Según el objetivo específico 1,** esta tesis logró evidenciar que la seguridad confidencial influye significativamente con la calidad de servicio de las redes LAN en la Municipalidad Distrital de Végueta, Huaura – 2025, debido a la clasificación de Pearson que devuelve un valor de 0.615, lo que indica una correlación positiva alta. Porque proteger la información evita riesgos y fallos en el sistema, mejorando el servicio de red.
3. **Según el objetivo específico 2,** esta tesis logró evidenciar que la seguridad integral influye significativamente con la calidad de servicio de las redes LAN en la Municipalidad Distrital de Végueta, Huaura – 2025, debido a la clasificación de Pearson que devuelve un valor de 0.623, lo que indica una correlación positiva alta. Porque aplicar medidas integrales de seguridad garantiza la continuidad y el buen desempeño de la red.
4. **Según el objetivo específico 3,** esta tesis logró evidenciar que la disponibilidad operativa influye significativamente con la calidad de servicio de las redes LAN en la Municipalidad Distrital de Végueta, Huaura – 2025, debido a la clasificación de Pearson que devuelve un valor de 0.751, lo que indica una correlación positiva alta. Porque mantener los equipos y servicios disponibles mejora la eficiencia y reduce interrupciones.
5. **Según el objetivo específico 4,** esta tesis logró evidenciar que el cumplimiento normativo influye significativamente con la calidad de servicio de las redes LAN en la Municipalidad Distrital de Végueta, Huaura – 2025, debido a la clasificación de Pearson que devuelve un valor de 0.771, lo que indica una correlación positiva

alta. Porque respetar las normas de seguridad fortalece la gestión y garantiza un servicio más confiable.

6.2. Recomendaciones

1. Se recomienda fortalecer el sistema de gestión de seguridad de la información mediante la actualización continua de políticas, procedimientos y controles tecnológicos que permitan optimizar la administración de los datos y los recursos informáticos. Además, se sugiere capacitar al personal en buenas prácticas de seguridad digital, con el fin de asegurar un servicio de red más estable, confiable y eficiente dentro de la Municipalidad Distrital de Végueta, Huaura.
2. Se recomienda implementar mecanismos más sólidos para proteger la confidencialidad de la información institucional, aplicando medidas como la encriptación de datos, la gestión segura de contraseñas y el control de accesos. Asimismo, se propone establecer protocolos internos de manejo de información sensible, garantizando la integridad del sistema y la confianza de los usuarios en el servicio de red.
3. Se recomienda adoptar una estrategia de seguridad integral que contemple la prevención, detección y respuesta ante posibles incidentes informáticos. Para ello, es necesario establecer políticas de monitoreo permanente, auditorías de seguridad y planes de contingencia, asegurando la continuidad operativa y el buen desempeño de las redes LAN de la institución.
4. Se recomienda mantener una adecuada disponibilidad operativa a través de la implementación de un plan de mantenimiento preventivo de los equipos, la actualización del software de red y la creación de sistemas de respaldo de datos. Además, se sugiere realizar revisiones periódicas que permitan anticipar fallas técnicas, evitando interrupciones y garantizando un servicio eficiente y continuo.
5. Se recomienda fortalecer el cumplimiento normativo mediante la adopción de estándares nacionales e internacionales en materia de seguridad informática, como la norma ISO/IEC 27001. Asimismo, se debe promover la cultura organizacional orientada al cumplimiento de las normas y políticas internas, lo que permitirá mejorar la gestión tecnológica, reducir vulnerabilidades y ofrecer un servicio de red más seguro y confiable.

CAPÍTULO VII. REFERENCIAS BIBLIOGRAFICAS

7.1. Fuentes documentales

Alvarado, C. (2022). *PENSEMOS*. Obtenido de Sistema de gestión de seguridad de la información: qué es y sus etapas: https://gestion.pensemos.com/

Avalos, A. (2020) *Migración de DNS y DHCP para la mejora de servicios en las redes Lan del grupo de tiendas Retail en el Perú – 2020* (Pregrado) Universidad Tecnológica del Perú. Lima-Perú

Berry, L. et al. (1989). Calidad de Servicio. Ediciones Diaz de Santos.

Cacuango, S. (2019). Evaluación de una Red LAN para el establecimiento de las Políticas de la Calidad de Servicio. Quito.

Calcina, M. (2023) *Diseño, optimización, implementación e integración de las redes LAN administrativa e industrial, para mejorar la calidad de servicio con tecnología cisco en la Unidad Minera San Rafael 2021* (Pregrado) Universidad Nacional Del Altiplano. Puno-Perú

Calder, A. y Watkins, S. (2010). *Information security risk management for ISO 27001/ISO 27002*. IT Governance Publishing.

Calder, A., y Watkins, S. (2012). *IT Governance: An International Guide to Data Security and ISO27001/ISO27002*. Kogan Page.

Cando, D. y Morales, F. (2020) *Implementación de una red LAN con acceso WAN, en la empresa GMS, administrada de acuerdo con la norma establecida por el Instituto SANS - SysAdmin Audit, Networking and Security Institute* (Posgrado) Universidad Tecnológica Israel. Quito-Ecuador

Castro, C. (2014). *Elaboración de un sistema de gestión de seguridad de la información (SGSI) para la empresa radical Cia. Ltda. en la ciudad de Quito para el año 2014* [Tesis de maestría, Universidad de las Américas]. Repositorio Digital Universidad De Las Américas. https://dspace.udla.edu.ec/handle/33000/3376

Castro, J. (2018). Implementación de la NTP ISO/IEC 27001:2014 para mejorar la gestión de la seguridad en los sistemas de información de la autoridad Portuaria Nacional, Callao - 2017. Lima - Callao.

Ccesa, M. (2017). Diseño de un sistema de seguridad de la información bajo la NTP ISO/IEC 27001:2014 para la Municipalidad Provincial de Huamanga, 2016. Ayacucho.

Diaz, V. (2021). Percepción de la implementación de la NTP-ISO/IEC 27001:2014 en base a la información documentada del gobierno central del Perú, año 2021. Lima.

Espinoza, M. (2022) *Elaboración de una guía de implementación de un SGSI para la Corporación Ecuatoriana para el Desarrollo de la Investigación y la Academia - CEDIA* (Pregrado) Universidad Politécnica Salesiana. Quito-Ecuador

Forouzan, B. A. (2007). *Data Communications and Networking* (4th ed.). McGraw-Hill.

Galindo, M. (2022) *Sistema de gestión de seguridad de la información y su relación con la calidad de servicio de las redes LAN en la Municipalidad Distrital de Ilabaya* (Pregrado) Universidad Privada De Tacna. Tacna – Perú

García, A., et al. (2011). *Seguridad informática*. Paraninfo, S.A

GeeksforGeeks. (2023). *Latency vs Jitter in Computer Networks*. Recuperado de https://www.geeksforgeeks.org

Harris, S. (2013). *CISSP All-in-One Exam Guide* (7th ed.). McGraw-Hill Education.

Humphreys, E. (2008). *Implementing the ISO/IEC 27001 Information Security Management System Standard*. Artech House.

International Organization for Standardization. (2013). *ISO/IEC 27001:2013 - Information technology — Security techniques — Information security management systems — Requirements*. ISO.

ISO/IEC. (2018). *ISO/IEC 27000: Information security management systems – Overview and vocabulary*. International Organization for Standardization.

Kurose, J. y Ross, K. (2013). *Computer Networking: A Top-Down Approach* (6th ed.). Pearson.

Ley l., N.et al. (2021). Eficacia y eficiencia de la seguridad de las redes LAN. Cantón Pasaje. Sociedad & Tecnología.

Martínez, V. (2023) *Sistema de gestión de seguridad de la información y la calidad de servicio de las redes en la Empresa Cerámica Lima S.A. - 2023* (Pregrado) Universidad José Carlos Mariátegui. Moquegua-Perú

Orellana, M. (2022) *Elaboración de una guía de implementación de un SGSI para la Corporación Ecuatoriana para el Desarrollo de la Investigación y la Academia - CEDIA* (Pregrado) Universidad Politécnica Salesiana. Cuenca-Ecuador

Peltier, T. (2005). *Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management*. Auerbach Publications.

Peterson, L. y Davie, B. (2007). *Computer Networks: A Systems Approach* (4th ed.). Morgan Kaufmann.

Pfleeger, C. y Pfleeger, S. (2012). *Security in Computing* (4th ed.). Prentice Hall.

Quinapallo, C. (2024) *Procedimiento de control de información registrada en los formularios de inclusión del Estándar común de reporte.* (Posgrado) Universidad Tecnológica Israel. Quito-Ecuador

Solms, R. von, y Niekerk, J. van. (2011). *Information Security: A Multidisciplinary Approach*. Springer.

Solms, R. von, y Niekerk, J. van. (2011). *Information Security: A Multidisciplinary Approach*. Springer.

Stallings, W. (2013). *Data and Computer Communications* (10th ed.). Pearson Education.

Suazo, J. (2024) *Sistema de gestión de seguridad de la información y la calidad de servicio de las redes en la Empresa Cerámica Lima S.A. - 2023* (Pregrado) Universidad Privada De Tacna. Tacna – Perú

Tanenbaum, A. y Wetherall, D. (2011). *Computer Networks* (5th ed.). Pearson Education.

Tanenbaum, A. y Wetherall, D. (2014). *Computer Networks* (5th ed.). Pearson.

Tipton, H. y Krause, M. (2007). *Information Security Management Handbook* (6th ed.). CRC Press.

Tøndel, I. et al. (2014). *Security in System-of-Systems: Foundations, Architectures and Applications*. Springer.

Trujillo, W. (2020). Diseño de controles y políticas para la seguridad de la información en la red LAN en el Hotel Pipaton. Barrancabermaja - Santander.

Universidad Rafael Belloso Chacín URBC. (2011). Criterios de calidad de servicio para la evaluacion de la gestion de redes LAN. Revista Electrónica de Estudios Telemáticos

Valenzuela, D. (2020) *Implementación de una red LAN con acceso WAN, en la empresa GMS, administrada de acuerdo con la norma establecida por el Instituto SANS - SysAdmin Audit, Networking and Security Institute* (Pregrado) Universidad Politécnica Salesiana. Quito-Ecuador

Venter, H. y Eloff, J. (2003). A taxonomy for information security technologies. *Computers & Security*, 22(4), 299–307.

von Solms, R., y von Solms, B. (2004). *Information Security Governance: A Model Based on the Direct–Control Perspective*. Computers & Security, 23(8), 638–646.

Whitman, M. E. y Mattord, H. J. (2011). *Principles of information security* (4th ed.). Cengage Learning.

Zheng, L. (2017). Diseño e implementación de una red LAN para la empresa Palinda. Quito.

ANEXOS

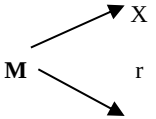
Anexo **N°1:** Matriz de consistencia

Anexo **N°2:** Instrumento de recolección de datos

Anexo N°3: Confiabilidad de Alfa Cronbach

Anexo N°4: Base de datos

Anexo N°1: Matriz de consistencia

PROBLEMAS	OBJETIVOS	HIPÓTESIS	VARIABLES	DIMENSIONES	INDICADORES	MÉTODO Y TÉCNICAS
Problema General ¿Cómo el sistema de gestión de seguridad de la información influye con la calidad de servicio de las redes LAN en la Municipalidad Distrital de Végueta, Huaura – 2025?	**Objetivo General** Conocer el sistema de gestión de seguridad de la información y su influencia con la calidad de servicio de las redes LAN en la Municipalidad Distrital de Végueta, Huaura – 2025.	**Hipótesis General** El sistema de gestión de seguridad de la información influye significativamente con la calidad de servicio de las redes LAN en la Municipalidad Distrital de Végueta, Huaura – 2025.	(X) Sistema de gestión de seguridad de la información	x.1.- seguridad confidencial x.2.- seguridad integral x.3.- disponibilidad operativa x.4.- cumplimiento normativo	X.1.1.- Acceso restringido a la información X.1.2.- Uso de contraseñas seguras X.1.3.- Control de usuarios y roles X.2.1.- Verificación de integridad X.2.2.- Registro de cambios X.2.3.- Prevención de modificaciones no autorizadas X.3.1.- Tiempo de disponibilidad de los sistemas X.3.2.- Planes de recuperación ante desastres X.3.3.- Mantenimiento periódico de infraestructura X.4.1.- Adopción de normativas X.4.2.- Auditorías de seguridad de la información X.4.3.- Políticas de seguridad implementadas	**Población** = 52 **Muestra** = 52 **Método**: Científico. **Técnicas:** **Para el acopio de Datos:** Encuesta **Instrumentos de recolección de datos:** Cuestionario. **Para el Procesamiento de datos.** Consistenciación, Codificación Tabulación de datos. **Técnicas para el análisis e interpretación de datos.** Paquete estadístico SPSS 24.0 Estadística descriptiva para cada variable. **Para presentación de datos** Cuadros, gráficos y figuras estadísticas. **Para el informe final:** Tipo de Investigación: Aplicada **Diseño de Investigación** Esquema propuesto por la EPIQ. **UNJFSC.** Nivel Correlacional Transeccional. 
Problemas Específicos: 1. ¿Cómo la seguridad confidencial influye con la calidad de servicio de las redes LAN en la Municipalidad Distrital de Végueta, Huaura – 2025? 2. ¿Cómo la seguridad integral influye con la calidad de servicio de las redes LAN en la Municipalidad Distrital de Végueta, Huaura – 2025?	**Objetivos Específicos:** 1. Conocer la seguridad confidencial y su influencia con la calidad de servicio de las redes LAN en la Municipalidad Distrital de Végueta, Huaura – 2025. 2. Conocer la seguridad integral y su influencia con la calidad de servicio de las redes LAN en la Municipalidad Distrital	**Hipótesis Específicos:** 1. 1. La seguridad confidencial influye significativamente con la calidad de servicio de las redes LAN en la Municipalidad Distrital de Végueta, Huaura – 2025. 2. La seguridad integral influye significativamente con la calidad de servicio de las redes LAN en la Municipalidad Distrital	(Y) La calidad de servicio de las redes LAN	y.1.- velocidad de transmisión y.2.- estabilidad de conexión y.3.- disponibilidad del servicio y.4.- seguridad de red	Y.1.1.- Tasa de transferencia de datos (Mbps) Y.1.2.- Tiempo de respuesta de la red Y.1.3.- Velocidad promedio de carga y descarga Y.2.1.- Frecuencia de caídas de red por semana Y.2.2.- Fluctuación del ancho de banda Y.2.3.- Variación en el tiempo de respuesta Y.3.1.- Tiempo total de red operativa Y.3.2.- Porcentaje de disponibilidad del servicio Y.3.3.- Tiempo medio de recuperación ante fallas	

3. ¿Cómo la disponibilidad operativa influye con la calidad de servicio de las redes LAN en la Municipalidad Distrital de Végueta, Huaura – 2025? 4. ¿Cómo el cumplimiento normativo influye con la calidad de servicio de las redes LAN en la Municipalidad Distrital de Végueta, Huaura – 2025??	de Végueta, Huaura – 2025. 3. Conocer la disponibilidad operativa y su influencia con la calidad de servicio de las redes LAN en la Municipalidad Distrital de Végueta, Huaura – 2025. 4. Conocer el cumplimiento normativo y su influencia con la calidad de servicio de las redes LAN en la Municipalidad Distrital de Végueta, Huaura – 2025.	de Végueta, Huaura – 2025. 3. La disponibilidad operativa influye significativamente con la calidad de servicio de las redes LAN en la Municipalidad Distrital de Végueta, Huaura – 2025. 4. El cumplimiento normativo influye significativamente con la calidad de servicio de las redes LAN en la Municipalidad Distrital de Végueta, Huaura – 2025.			Y.4.1.- Número de accesos no autorizados detectados Y.4.2.- Presencia de antivirus/firewall activo en la red Y.4.3.- Número de incidentes de seguridad reportados	

Anexo N°2: Instrumento de recolección de datos

Estimado(a) colaborador(a):

El presente cuestionario tiene como finalidad recopilar información para Conocer el sistema de gestión de seguridad de la información y su influencia con la calidad de servicio de las redes LAN en la Municipalidad Distrital de Végueta, Huaura – 2025. Su participación es fundamental, ya que sus respuestas permitirán identificar las características clave relacionadas con la resistencia y el comportamiento estructural, y proponer mejoras que optimicen el diseño y la seguridad del Distrital de Végueta.

Le solicitamos responder de manera objetiva, honesta y sincera. Queremos asegurarle que sus respuestas serán tratadas con estricta confidencialidad y utilizadas exclusivamente para fines académicos.

Instrucciones:

- Cada ítem incluye cinco alternativas de respuesta que representan con qué frecuencia o en qué medida usted está de acuerdo con la afirmación planteada.
- Por favor, lea con atención cada enunciado y marque **una sola respuesta** con una equis (x) en la opción que mejor refleje su experiencia o percepción, utilizando la escala proporcionada.

Escala de respuestas:

- Siempre
- Casi siempre
- A veces
- Casi nunca
- Nunca

Agradecemos de antemano su valiosa participación en este estudio, que contribuirá a optimizar los procesos y mejorar el desempeño productivo de nuestra empresa.

¡Muchas gracias por su colaboración!

CUESTIONARIO SOBRE LA VARIABLE: "Sistema de gestión de seguridad de la información"

Escala valorativa

Nunca	Casi nunca	A veces	Casi siempre	Siempre
1	2	3	4	5

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (X)						
N°	**X.1. Seguridad confidencial**	**N.**	**C.N..**	**A.V.**	**C.S.**	**S.**
01	¿Se restringe el acceso a la información según el nivel de autorización del usuario?					
02	¿Utiliza contraseñas seguras para ingresar a los sistemas informáticos?					
03	¿El sistema controla adecuadamente los roles y permisos de los usuarios?					
	X.2. Seguridad integral					
04	¿Se verifica la integridad de los datos almacenados o procesados en los sistemas?					
05	¿Existen registros detallados de los cambios realizados en los sistemas o bases de datos?					
06	¿Se cuenta con medidas efectivas para prevenir modificaciones no autorizadas?					
	X.3. Disponibilidad operativa					
07	¿Los sistemas informáticos están disponibles durante el horario laboral sin interrupciones?					
08	¿Existe un plan de recuperación ante desastres que garantice la continuidad del servicio?					
09	¿Se realiza mantenimiento periódico a la infraestructura tecnológica?					
	X.4. Cumplimiento normativo					
10	¿La institución ha adoptado normas reconocidas de seguridad de la información?					
11	¿Se realizan auditorías periódicas para verificar el cumplimiento de políticas de seguridad?					
12	¿Se han implementado políticas formales de seguridad de la información?					

CUESTIONARIO SOBRE LA VARIABLE: "La calidad de servicio de las redes LAN"

Escala valorativa

Nunca	Casi nunca	A veces	Casi siempre	Siempre
1	2	3	4	5

LA CALIDAD DE SERVICIO DE LAS REDES LAN (Y)						
	Y.1. Velocidad de transmisión	**N.**	**C.N..**	**A.V.**	**C.S.**	**S.**
01	¿La tasa de transferencia de datos (subida/bajada) es adecuada para sus actividades laborales?					
02	¿El tiempo de respuesta de la red es rápido al acceder a páginas o servicios?					
03	¿La velocidad promedio de carga y descarga se mantiene constante?					
	Y.2. Estabilidad de conexión					
04	¿Con qué frecuencia experimenta caídas en la conexión de red?					
05	¿Ha notado fluctuaciones en el ancho de banda durante su jornada laboral?					
06	¿Experimenta variaciones notables en el tiempo de respuesta al utilizar la red?					
	Y.3. Disponibilidad del servicio					
07	¿La red LAN se mantiene operativa durante la mayor parte del día?					
08	¿El servicio de red presenta un porcentaje de disponibilidad cercano al 100%?					
09	¿Después de una falla de red, el servicio se recupera en poco tiempo?					
	Y.4. Seguridad de red					
10	¿Se detectan e informan accesos no autorizados a la red?					
11	¿La red LAN cuenta con antivirus y firewall activo funcionando correctamente?					
12	¿Con qué frecuencia se reportan incidentes de seguridad en la red?					

Anexo N°3: Confiabilidad de Alfa Cronbach

La confiabilidad de los instrumentos se evaluó mediante el coeficiente alfa de Cronbach, que es una medida comúnmente utilizada para determinar la consistencia interna de los ítems de un instrumento.

Midiendo los ítems de los cuestionarios

Estadísticos de fiabilidad del sistema de gestión de seguridad de la información

Alfa de Cronbach	N de elementos
,912	12

estadísticos de fiabilidad de la calidad de servicio de las redes LAN

Alfa de Cronbach	N de elementos
,899	12

Para ambas variables, según el coeficiente alfa de Cronbach indica una excelente consistencia interna entre los ítems del cuestionario. Este resultado indica que el instrumento de medición fue confiable para evaluar ambas variables con respecto a los datos en la muestra de estudio.

Anexo N°4: Base de datos

N	Sistema de gestión de seguridad de la información																				ST1	X
	Seguridad confidencial					Seguridad integral					Disponibilidad operativa					Cumplimiento normativo						
	1	2	3	S1	D1	4	5	6	S2	D2	7	8	9	S3	D3	10	11	12	S4	D4		
1	4	1	5	10	A Veces	4	4	1	9	A Veces	4	4	1	9	A Veces	4	1	1	6	Casi Nunca	34	A Veces
2	4	1	4	9	A Veces	4	4	1	9	A Veces	4	4	1	9	A Veces	4	1	1	6	Casi Nunca	33	Casi Nunca
3	2	2	4	8	A Veces	5	2	5	12	Casi Siempre	5	2	5	12	Casi Siempre	2	2	2	6	Casi Nunca	38	A Veces
4	1	5	2	8	A Veces	1	5	5	11	Casi Siempre	1	5	5	11	Casi Siempre	1	5	5	11	Casi Siempre	41	A Veces
5	5	5	1	11	Casi Siempre	5	5	5	15	Siempre	5	5	5	15	Siempre	5	5	5	15	Siempre	56	Casi Siempre
6	3	2	5	10	A Veces	5	5	5	15	Siempre	3	2	2	7	Casi Nunca	3	2	2	7	Casi Nunca	39	A Veces
7	5	3	3	11	Casi Siempre	5	3	3	11	Casi Siempre	5	3	3	11	Casi Siempre	5	3	3	11	Casi Siempre	44	A Veces
8	2	1	5	8	A Veces	2	1	1	4	Nunca	2	1	1	4	Nunca	2	1	1	4	Nunca	20	Nunca
9	4	3	2	9	A Veces	4	3	3	10	A Veces	4	3	3	10	A Veces	4	3	3	10	A Veces	39	A Veces
10	5	2	4	11	Casi Siempre	5	2	2	9	A Veces	5	2	2	9	A Veces	5	2	2	9	A Veces	38	A Veces
11	1	3	5	9	A Veces	1	3	3	7	Casi Nunca	1	3	3	7	Casi Nunca	1	3	3	7	Casi Nunca	30	Casi Nunca
12	2	1	1	4	Nunca	2	1	1	4	Nunca	2	1	1	4	Nunca	2	1	1	4	Nunca	16	Nunca
13	2	2	2	6	Casi Nunca	4	4	4	12	Casi Siempre	2	2	2	6	Casi Nunca	2	2	2	6	Casi Nunca	30	Casi Nunca
14	2	3	2	7	Casi Nunca	2	3	3	8	A Veces	2	3	3	8	A Veces	2	3	3	8	A Veces	31	Casi Nunca
15	3	4	2	9	A Veces	3	4	4	11	Casi Siempre	3	4	4	11	Casi Siempre	3	4	4	11	Casi Siempre	42	A Veces
16	5	5	3	13	Casi Siempre	5	5	5	15	Siempre	5	5	5	15	Siempre	5	5	5	15	Siempre	58	Siempre
17	2	3	5	10	A Veces	5	3	5	13	Casi Siempre	5	3	5	13	Casi Siempre	2	3	3	8	A Veces	44	A Veces
18	3	2	2	7	Casi Nunca	5	2	5	12	Casi Siempre	5	2	5	12	Casi Siempre	3	2	2	7	Casi Nunca	38	A Veces
19	4	1	3	8	A Veces	4	1	1	6	Casi Nunca	4	1	1	6	Casi Nunca	4	1	1	6	Casi Nunca	26	Casi Nunca
20	5	2	4	11	Casi Siempre	5	2	2	9	A Veces	5	2	2	9	A Veces	5	2	2	9	A Veces	38	A Veces
21	2	3	5	10	A Veces	2	5	5	12	Casi Siempre	2	3	3	8	A Veces	2	3	3	8	A Veces	38	A Veces

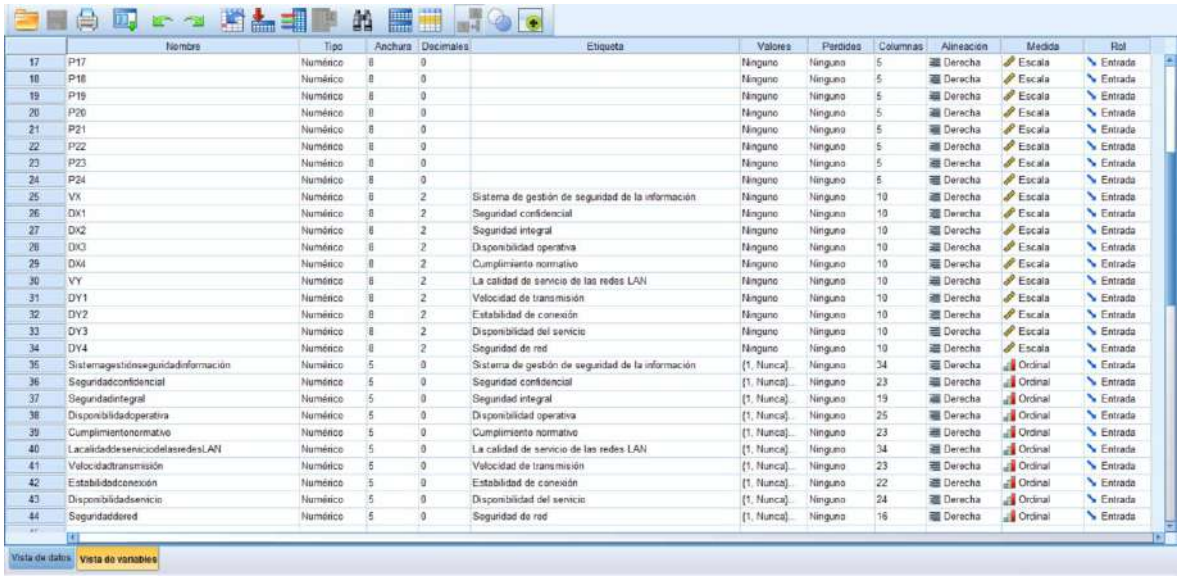
22	5	5	2	**12**	Casi Siempre	5	5	5	**15**	Siempre	5	5	5	**15**	Siempre	5	5	5	**15**	Siempre	57	Casi Siempre
23	3	1	5	**9**	A Veces	3	1	1	**5**	Casi Nunca	3	1	1	**5**	Casi Nunca	3	1	1	**5**	Casi Nunca	24	Casi Nunca
24	4	1	5	**10**	A Veces	4	1	1	**6**	Casi Nunca	4	1	1	**6**	Casi Nunca	4	1	1	**6**	Casi Nunca	28	Casi Nunca
25	4	1	4	**9**	A Veces	4	1	1	**6**	Casi Nunca	4	1	1	**6**	Casi Nunca	4	1	1	**6**	Casi Nunca	27	Casi Nunca
26	5	5	4	**14**	Siempre	5	5	5	**15**	Siempre	5	5	5	**15**	Siempre	5	5	5	**15**	Siempre	59	Siempre
27	1	5	5	**11**	Casi Siempre	1	5	5	**11**	Casi Siempre	1	5	5	**11**	Casi Siempre	1	5	5	**11**	Casi Siempre	44	A Veces
28	5	5	1	**11**	Casi Siempre	5	5	5	**15**	Siempre	5	5	5	**15**	Siempre	5	5	5	**15**	Siempre	56	Casi Siempre
29	3	2	5	**10**	A Veces	3	2	2	**7**	Casi Nunca	3	2	2	**7**	Casi Nunca	3	2	2	**7**	Casi Nunca	31	Casi Nunca
30	5	3	3	**11**	Casi Siempre	5	3	3	**11**	Casi Siempre	5	3	3	**11**	Casi Siempre	5	3	3	**11**	Casi Siempre	44	A Veces
31	2	1	5	**8**	A Veces	2	1	1	**4**	Nunca	2	1	1	**4**	Nunca	2	1	1	**4**	Nunca	20	Nunca
32	4	3	2	**9**	A Veces	4	3	5	**12**	Casi Siempre	4	3	5	**12**	Casi Siempre	4	3	3	**10**	A Veces	43	A Veces
33	2	2	4	**8**	A Veces	2	2	2	**6**	Casi Nunca	2	2	2	**6**	Casi Nunca	2	2	2	**6**	Casi Nunca	26	Casi Nunca
34	3	5	2	**10**	A Veces	3	5	5	**13**	Casi Siempre	3	5	5	**13**	Casi Siempre	3	5	5	**13**	Casi Siempre	49	Casi Siempre
35	1	3	3	**7**	Casi Nunca	1	3	3	**7**	Casi Nunca	1	3	3	**7**	Casi Nunca	1	3	3	**7**	Casi Nunca	28	Casi Nunca
36	2	1	1	**4**	Nunca	2	1	1	**4**	Nunca	2	1	1	**4**	Nunca	2	1	1	**4**	Nunca	16	Nunca
37	5	5	5	**15**	Siempre	5	5	5	**15**	Siempre	5	5	5	**15**	Siempre	5	5	5	**15**	Siempre	60	Siempre
38	2	3	5	**10**	A Veces	2	3	3	**8**	A Veces	2	3	3	**8**	A Veces	2	3	3	**8**	A Veces	34	A Veces
39	3	4	2	**9**	A Veces	3	4	4	**11**	Casi Siempre	3	4	4	**11**	Casi Siempre	3	4	4	**11**	Casi Siempre	42	A Veces
40	5	5	5	**15**	Siempre	5	5	5	**15**	Siempre	5	5	5	**15**	Siempre	5	5	5	**15**	Siempre	60	Siempre
41	2	3	5	**10**	A Veces	2	4	4	**10**	A Veces	2	3	3	**8**	A Veces	2	3	3	**8**	A Veces	36	A Veces
42	3	2	2	**7**	Casi Nunca	3	2	2	**7**	Casi Nunca	3	2	2	**7**	Casi Nunca	3	2	2	**7**	Casi Nunca	28	Casi Nunca
43	1	1	3	**5**	Casi Nunca	1	1	1	**3**	Nunca	1	1	1	**3**	Nunca	1	1	1	**3**	Nunca	14	Nunca
44	2	5	1	**8**	A Veces	2	5	5	**12**	Casi Siempre	2	5	5	**12**	Casi Siempre	2	5	5	**12**	Casi Siempre	44	A Veces
45	2	3	2	**7**	Casi Nunca	2	3	3	**8**	A Veces	2	3	3	**8**	A Veces	2	3	3	**8**	A Veces	31	Casi Nunca
46	5	5	2	**12**	Casi Siempre	5	5	5	**15**	Siempre	5	5	5	**15**	Siempre	5	5	5	**15**	Siempre	57	Casi Siempre
47	1	1	5	**7**	Casi Nunca	1	1	1	**3**	Nunca	1	1	1	**3**	Nunca	1	1	1	**3**	Nunca	16	Nunca
48	4	1	1	**6**	Casi Nunca	4	4	4	**12**	Casi Siempre	4	1	1	**6**	Casi Nunca	4	1	1	**6**	Casi Nunca	30	Casi Nunca

49	4	1	4	**9**	A Veces	4	1	1	**6**	Casi Nunca	4	1	1	**6**	Casi Nunca	4	1	1	**6**	Casi Nunca	27	Casi Nunca
50	2	2	4	**8**	A Veces	2	2	2	**6**	Casi Nunca	2	2	2	**6**	Casi Nunca	2	2	2	**6**	Casi Nunca	26	Casi Nunca
51	5	5	2	**12**	Casi Siempre	5	5	5	**15**	Siempre	5	5	5	**15**	Siempre	5	5	5	**15**	Siempre	57	Casi Siempre
52	5	5	5	**15**	Siempre	5	5	5	**15**	Siempre	5	5	5	**15**	Siempre	5	5	5	**15**	Siempre	60	Siempre

N	**La calidad de servicio de las redes LAN**																					
	Velocidad de transmisión					**Estabilidad de conexión**					**Disponibilidad del servicio**					**Seguridad de red**					**ST2**	**Y**
	13	**14**	**15**	**S1**	**D1**	**16**	**17**	**18**	**S2**	**D2**	**19**	**20**	**21**	**S3**	**D3**	**22**	**23**	**24**	**S4**	**D4**		
1	1	3	4	**8**	A Veces	1	3	5	**9**	A Veces	3	4	2	**9**	A Veces	3	4	1	**8**	A Veces	**34**	A Veces
2	1	4	4	**9**	A Veces	1	4	1	**6**	Casi Nunca	4	4	3	**11**	Casi Siempre	4	4	1	**9**	A Veces	**35**	A Veces
3	2	5	2	**9**	A Veces	2	5	3	**10**	A Veces	5	2	2	**9**	A Veces	5	2	2	**9**	A Veces	**37**	A Veces
4	5	5	5	**15**	Siempre	5	5	1	**11**	Casi Siempre	5	5	5	**15**	Siempre	5	5	5	**15**	Siempre	**56**	Casi Siempre
5	5	2	5	**12**	Casi Siempre	5	2	3	**10**	A Veces	2	5	1	**8**	A Veces	2	5	5	**12**	Casi Siempre	**42**	A Veces
6	2	1	3	**6**	Casi Nunca	2	1	2	**5**	Casi Nunca	1	3	3	**7**	Casi Nunca	1	3	2	**6**	Casi Nunca	**24**	Casi Nunca
7	3	2	5	**10**	A Veces	3	2	3	**8**	A Veces	2	5	1	**8**	A Veces	2	5	3	**10**	A Veces	**36**	A Veces
8	1	3	2	**6**	Casi Nunca	1	3	3	**7**	Casi Nunca	3	2	3	**8**	A Veces	3	2	1	**6**	Casi Nunca	**27**	Casi Nunca
9	3	5	4	**12**	Casi Siempre	3	5	3	**11**	Casi Siempre	5	4	2	**11**	Casi Siempre	5	4	3	**12**	Casi Siempre	**46**	Casi Siempre
10	2	1	5	**8**	A Veces	2	1	1	**4**	Nunca	1	5	3	**9**	A Veces	1	5	2	**8**	A Veces	**29**	Casi Nunca
11	3	1	1	**5**	Casi Nunca	3	1	2	**6**	Casi Nunca	1	1	3	**5**	Casi Nunca	1	1	3	**5**	Casi Nunca	**21**	Nunca
12	1	1	2	**4**	Nunca	1	1	5	**7**	Casi Nunca	1	2	3	**6**	Casi Nunca	1	2	1	**4**	Nunca	**21**	Nunca
13	2	2	2	**6**	Casi Nunca	2	2	5	**9**	A Veces	2	2	1	**5**	Casi Nunca	2	2	2	**6**	Casi Nunca	**26**	Casi Nunca
14	3	5	2	**10**	A Veces	3	5	3	**11**	Casi Siempre	5	2	2	**9**	A Veces	5	2	3	**10**	A Veces	**40**	A Veces
15	5	5	5	**15**	Siempre	5	5	5	**15**	Siempre	5	5	5	**15**	Siempre	5	5	5	**15**	Siempre	**60**	Siempre
16	5	5	5	**15**	Siempre	5	5	5	**15**	Siempre	5	5	5	**15**	Siempre	5	5	5	**15**	Siempre	**60**	Siempre
17	3	3	2	**8**	A Veces	3	3	1	**7**	Casi Nunca	3	2	3	**8**	A Veces	3	2	3	**8**	A Veces	**31**	Casi Nunca
18	2	1	3	**6**	Casi Nunca	2	1	3	**6**	Casi Nunca	1	3	2	**6**	Casi Nunca	1	3	2	**6**	Casi Nunca	**24**	Casi Nunca

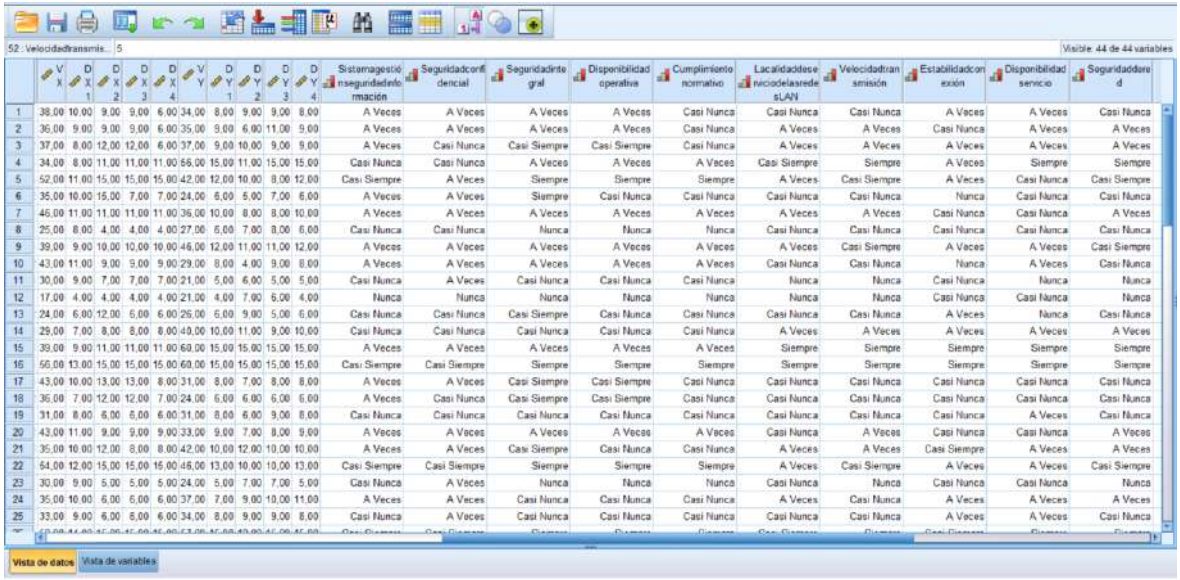
19	1	3	4	**8**	A Veces	1	3	2	**6**	Casi Nunca	3	4	2	**9**	A Veces	3	4	1	**8**	A Veces	**31**	Casi Nunca
20	2	2	5	**9**	A Veces	2	2	3	**7**	Casi Nunca	2	5	1	**8**	A Veces	2	5	2	**9**	A Veces	**33**	Casi Nunca
21	3	5	2	**10**	A Veces	3	5	4	**12**	Casi Siempre	5	2	3	**10**	A Veces	5	2	3	**10**	A Veces	**42**	A Veces
22	5	3	5	**13**	Casi Siempre	5	3	2	**10**	A Veces	3	5	2	**10**	A Veces	3	5	5	**13**	Casi Siempre	**46**	Casi Siempre
23	1	1	3	**5**	Casi Nunca	1	1	5	**7**	Casi Nunca	1	3	3	**7**	Casi Nunca	1	3	1	**5**	Casi Nunca	**24**	Casi Nunca
24	1	2	4	**7**	Casi Nunca	5	2	2	**9**	A Veces	2	4	4	**10**	A Veces	2	4	5	**11**	Casi Siempre	**37**	A Veces
25	1	3	4	**8**	A Veces	1	3	5	**9**	A Veces	3	4	2	**9**	A Veces	3	4	1	**8**	A Veces	**34**	A Veces
26	5	5	5	**15**	Siempre	5	5	2	**12**	Casi Siempre	5	5	5	**15**	Siempre	5	5	5	**15**	Siempre	**57**	Casi Siempre
27	5	5	1	**11**	Casi Siempre	5	5	5	**15**	Siempre	5	1	2	**8**	A Veces	5	1	5	**11**	Casi Siempre	**45**	A Veces
28	5	5	5	**15**	Siempre	5	5	5	**15**	Siempre	5	5	5	**15**	Siempre	5	5	5	**15**	Siempre	**60**	Siempre
29	2	2	3	**7**	Casi Nunca	2	2	4	**8**	A Veces	2	3	2	**7**	Casi Nunca	2	3	2	**7**	Casi Nunca	**29**	Casi Nunca
30	3	3	5	**11**	Casi Siempre	3	3	3	**9**	A Veces	3	5	5	**13**	Casi Siempre	3	5	3	**11**	Casi Siempre	**44**	A Veces
31	1	1	2	**4**	Nunca	1	1	5	**7**	Casi Nunca	1	2	3	**6**	Casi Nunca	1	2	1	**4**	Nunca	**21**	Nunca
32	3	3	4	**10**	A Veces	3	3	2	**8**	A Veces	3	4	4	**11**	Casi Siempre	3	4	3	**10**	A Veces	**39**	A Veces
33	2	2	2	**6**	Casi Nunca	2	2	3	**7**	Casi Nunca	2	2	3	**7**	Casi Nunca	2	2	2	**6**	Casi Nunca	**26**	Casi Nunca
34	5	5	3	**13**	Casi Siempre	5	5	3	**13**	Casi Siempre	5	3	5	**13**	Casi Siempre	5	3	5	**13**	Casi Siempre	**52**	Casi Siempre
35	3	3	1	**7**	Casi Nunca	3	3	4	**10**	A Veces	3	1	2	**6**	Casi Nunca	3	1	3	**7**	Casi Nunca	**30**	Casi Nunca
36	1	1	2	**4**	Nunca	1	1	2	**4**	Nunca	1	2	3	**6**	Casi Nunca	1	2	1	**4**	Nunca	**18**	Nunca
37	2	2	2	**6**	Casi Nunca	2	2	5	**9**	A Veces	2	2	3	**7**	Casi Nunca	2	2	2	**6**	Casi Nunca	**28**	Casi Nunca
38	3	3	2	**8**	A Veces	3	3	3	**9**	A Veces	3	2	4	**9**	A Veces	3	2	3	**8**	A Veces	**34**	A Veces
39	4	4	3	**11**	Casi Siempre	4	4	4	**12**	Casi Siempre	4	3	2	**9**	A Veces	4	3	4	**11**	Casi Siempre	**43**	A Veces
40	5	5	5	**15**	Siempre	5	5	2	**12**	Casi Siempre	5	5	5	**15**	Siempre	5	5	5	**15**	Siempre	**57**	Casi Siempre
41	3	3	2	**8**	A Veces	3	3	3	**9**	A Veces	3	2	3	**8**	A Veces	3	2	3	**8**	A Veces	**33**	Casi Nunca
42	2	2	3	**7**	Casi Nunca	2	2	2	**6**	Casi Nunca	2	3	4	**9**	A Veces	2	3	2	**7**	Casi Nunca	**29**	Casi Nunca
43	1	1	4	**6**	Casi Nunca	1	1	1	**3**	Nunca	1	4	2	**7**	Casi Nunca	1	4	1	**6**	Casi Nunca	**22**	Casi Nunca
44	5	2	2	**9**	A Veces	5	2	2	**9**	A Veces	2	2	3	**7**	Casi Nunca	2	2	5	**9**	A Veces	**34**	A Veces
45	3	3	2	**8**	A Veces	3	3	3	**9**	A Veces	3	2	2	**7**	Casi Nunca	3	2	3	**8**	A Veces	**32**	Casi Nunca
46	5	5	5	**15**	Siempre	5	5	5	**15**	Siempre	5	5	5	**15**	Siempre	5	5	5	**15**	Siempre	**60**	Siempre
47	1	1	5	**7**	Casi Nunca	1	1	5	**7**	Casi Nunca	1	5	5	**11**	Casi Siempre	1	5	1	**7**	Casi Nunca	**32**	Casi Nunca
48	5	1	4	**10**	A Veces	1	1	1	**3**	Nunca	1	4	2	**7**	Casi Nunca	1	4	1	**6**	Casi Nunca	**26**	Casi Nunca

49	1	1	4	**6**	Casi Nunca	1	1	5	**7**	Casi Nunca	1	4	2	**7**	Casi Nunca	1	4	5	**10**	A Veces	**30**	Casi Nunca
50	2	2	2	**6**	Casi Nunca	2	2	2	**6**	Casi Nunca	2	2	2	**6**	Casi Nunca	2	2	2	**6**	Casi Nunca	**24**	Casi Nunca
51	5	5	1	**11**	Casi Siempre	5	5	5	**15**	Siempre	5	1	3	**9**	A Veces	5	1	5	**11**	Casi Siempre	**46**	Casi Siempre
52	5	5	5	**15**	Siempre	5	5	5	**15**	Siempre	5	5	5	**15**	Siempre	5	5	5	**15**	Siempre	**60**	Siempre



	Nombre	Tipo	Anchura	Decimales	Etiqueta	Valores	Perdidos	Columnas	Alineación	Medida	Rol
17	P17	Numérico	8	0		Ninguno	Ninguno	5	Derecha	Escala	Entrada
18	P18	Numérico	8	0		Ninguno	Ninguno	5	Derecha	Escala	Entrada
19	P19	Numérico	8	0		Ninguno	Ninguno	5	Derecha	Escala	Entrada
20	P20	Numérico	8	0		Ninguno	Ninguno	5	Derecha	Escala	Entrada
21	P21	Numérico	8	0		Ninguno	Ninguno	5	Derecha	Escala	Entrada
22	P22	Numérico	8	0		Ninguno	Ninguno	5	Derecha	Escala	Entrada
23	P23	Numérico	8	0		Ninguno	Ninguno	5	Derecha	Escala	Entrada
24	P24	Numérico	8	0		Ninguno	Ninguno	5	Derecha	Escala	Entrada
25	VX	Numérico	8	2	Sistema de gestión de seguridad de la información	Ninguno	Ninguno	10	Derecha	Escala	Entrada
26	DX1	Numérico	8	2	Seguridad confidencial	Ninguno	Ninguno	10	Derecha	Escala	Entrada
27	DX2	Numérico	8	2	Seguridad integral	Ninguno	Ninguno	10	Derecha	Escala	Entrada
28	DX3	Numérico	8	2	Disponibilidad operativa	Ninguno	Ninguno	10	Derecha	Escala	Entrada
29	DX4	Numérico	8	2	Cumplimiento normativo	Ninguno	Ninguno	10	Derecha	Escala	Entrada
30	VY	Numérico	8	2	La calidad de servicio de las redes LAN	Ninguno	Ninguno	10	Derecha	Escala	Entrada
31	DY1	Numérico	8	2	Velocidad de transmisión	Ninguno	Ninguno	10	Derecha	Escala	Entrada
32	DY2	Numérico	8	2	Estabilidad de conexión	Ninguno	Ninguno	10	Derecha	Escala	Entrada
33	DY3	Numérico	8	2	Disponibilidad del servicio	Ninguno	Ninguno	10	Derecha	Escala	Entrada
34	DY4	Numérico	8	2	Seguridad de red	Ninguno	Ninguno	10	Derecha	Escala	Entrada
35	Sistemagestióninseguridadinformación	Numérico	5	0	Sistema de gestión de seguridad de la información	{1, Nunca}...	Ninguno	34	Derecha	Ordinal	Entrada
36	Seguridadconfidencial	Numérico	5	0	Seguridad confidencial	{1, Nunca}...	Ninguno	23	Derecha	Ordinal	Entrada
37	Seguridadintegral	Numérico	5	0	Seguridad integral	{1, Nunca}...	Ninguno	19	Derecha	Ordinal	Entrada
38	Disponibilidadoperativa	Numérico	5	0	Disponibilidad operativa	{1, Nunca}...	Ninguno	25	Derecha	Ordinal	Entrada
39	Cumplimientonormativo	Numérico	5	0	Cumplimiento normativo	{1, Nunca}...	Ninguno	23	Derecha	Ordinal	Entrada
40	LacalidaddeservicíodelasredesLAN	Numérico	5	0	La calidad de servicio de las redes LAN	{1, Nunca}...	Ninguno	34	Derecha	Ordinal	Entrada
41	Velocidadtransmisión	Numérico	5	0	Velocidad de transmisión	{1, Nunca}...	Ninguno	23	Derecha	Ordinal	Entrada
42	Estabilidadconexión	Numérico	5	0	Estabilidad de conexión	{1, Nunca}...	Ninguno	22	Derecha	Ordinal	Entrada
43	Disponibilidadservicio	Numérico	5	0	Disponibilidad del servicio	{1, Nunca}...	Ninguno	24	Derecha	Ordinal	Entrada
44	Seguridaddered	Numérico	5	0	Seguridad de red	{1, Nunca}...	Ninguno	16	Derecha	Ordinal	Entrada

Vista de datos | Vista de variables



52 : Velocidadtransmis... 5

Visible: 44 de 44 variables

	VX	DX1	DX2	DX3	DX4	VY	DY1	DY2	DY3	DY4	Sistemagestióninseguridadeinformación	Seguridadconfidencial	Seguridadintegral	Disponibilidadoperativa	Cumplimientonormativo	Lacalidaddeservicíodelasredes LAN	Velocidadtransmisión	Estabilidadconexión	Disponibilidadservicio	Seguridaddered
1	38,00	10,00	9,00	9,00	6,00	34,00	8,00	9,00	9,00	8,00	A Veces	A Veces	A Veces	A Veces	Casi Nunca	Casi Nunca	Casi Nunca	A Veces	A Veces	Casi Nunca
2	36,00	9,00	9,00	9,00	6,00	35,00	9,00	6,00	11,00	9,00	A Veces	A Veces	A Veces	A Veces	Casi Nunca	A Veces	A Veces	Casi Nunca	A Veces	A Veces
3	37,00	8,00	12,00	12,00	6,00	37,00	9,00	10,00	9,00	9,00	A Veces	Casi Nunca	Casi Siempre	Casi Siempre	Casi Nunca	A Veces	A Veces	A Veces	A Veces	A Veces
4	34,00	8,00	11,00	11,00	11,00	56,00	15,00	11,00	15,00	15,00	Casi Nunca	Casi Nunca	A Veces	A Veces	A Veces	Casi Siempre	Siempre	A Veces	Siempre	Siempre
5	52,00	11,00	15,00	15,00	15,00	42,00	12,00	10,00	8,00	12,00	Casi Siempre	A Veces	Siempre	Siempre	Siempre	A Veces	Casi Siempre	A Veces	Casi Nunca	Casi Siempre
6	35,00	10,00	15,00	7,00	7,00	24,00	6,00	5,00	7,00	6,00	A Veces	A Veces	Siempre	Casi Nunca	Casi Nunca	Casi Nunca	Casi Nunca	Nunca	Casi Nunca	Casi Nunca
7	46,00	11,00	11,00	11,00	11,00	36,00	10,00	8,00	8,00	10,00	A Veces	A Veces	A Veces	A Veces	A Veces	A Veces	A Veces	Casi Nunca	Casi Nunca	A Veces
8	25,00	8,00	4,00	4,00	4,00	27,00	6,00	7,00	8,00	6,00	Casi Nunca	Casi Nunca	Nunca	Nunca	Nunca	Casi Nunca	Casi Nunca	Casi Nunca	Casi Nunca	Casi Nunca
9	39,00	9,00	10,00	10,00	10,00	46,00	12,00	11,00	11,00	12,00	A Veces	A Veces	A Veces	A Veces	A Veces	A Veces	Casi Siempre	A Veces	A Veces	Casi Siempre
10	43,00	11,00	9,00	9,00	9,00	29,00	8,00	4,00	9,00	8,00	A Veces	A Veces	A Veces	A Veces	A Veces	Casi Nunca	Casi Nunca	Nunca	A Veces	Casi Nunca
11	30,00	9,00	7,00	7,00	7,00	21,00	5,00	6,00	5,00	5,00	Casi Nunca	A Veces	Casi Nunca	Casi Nunca	Casi Nunca	Nunca	Nunca	Casi Nunca	Nunca	Nunca
12	17,00	4,00	4,00	4,00	4,00	21,00	4,00	7,00	6,00	4,00	Nunca	Nunca	Nunca	Nunca	Nunca	Nunca	Nunca	Casi Nunca	Casi Nunca	Nunca
13	24,00	6,00	12,00	6,00	6,00	26,00	6,00	9,00	5,00	6,00	Casi Nunca	Casi Nunca	Casi Siempre	Casi Nunca	Casi Nunca	Casi Nunca	Casi Nunca	A Veces	Nunca	Casi Nunca
14	29,00	7,00	8,00	8,00	8,00	40,00	10,00	11,00	9,00	10,00	Casi Nunca	Casi Nunca	Casi Nunca	Casi Nunca	Casi Nunca	A Veces	A Veces	A Veces	A Veces	A Veces
15	39,00	9,00	11,00	11,00	11,00	60,00	15,00	15,00	15,00	15,00	A Veces	A Veces	A Veces	A Veces	A Veces	Siempre	Siempre	Siempre	Siempre	Siempre
16	56,00	13,00	15,00	15,00	15,00	60,00	15,00	15,00	15,00	15,00	Casi Siempre	Casi Siempre	Siempre	Siempre	Siempre	Siempre	Siempre	Siempre	Siempre	Siempre
17	43,00	10,00	13,00	13,00	8,00	31,00	8,00	7,00	8,00	8,00	A Veces	A Veces	Casi Siempre	Casi Siempre	Casi Nunca	Casi Nunca	Casi Nunca	Casi Nunca	Casi Nunca	Casi Nunca
18	36,00	7,00	12,00	12,00	7,00	24,00	6,00	6,00	6,00	6,00	A Veces	Casi Nunca	Casi Siempre	Casi Siempre	Casi Nunca	Casi Nunca	Casi Nunca	Casi Nunca	Casi Nunca	Casi Nunca
19	31,00	8,00	6,00	6,00	6,00	31,00	8,00	6,00	9,00	8,00	Casi Nunca	Casi Nunca	Casi Nunca	Casi Nunca	Casi Nunca	Casi Nunca	Casi Nunca	Casi Nunca	A Veces	Casi Nunca
20	43,00	11,00	9,00	9,00	9,00	33,00	9,00	7,00	8,00	9,00	A Veces	A Veces	A Veces	A Veces	A Veces	Casi Nunca	A Veces	Casi Nunca	Casi Nunca	A Veces
21	35,00	10,00	12,00	8,00	8,00	42,00	10,00	12,00	10,00	10,00	A Veces	A Veces	Casi Siempre	Casi Nunca	Casi Nunca	A Veces	A Veces	Casi Siempre	A Veces	A Veces
22	64,00	12,00	15,00	15,00	15,00	46,00	13,00	10,00	10,00	13,00	Casi Siempre	Casi Siempre	Siempre	Siempre	Siempre	A Veces	Casi Siempre	A Veces	A Veces	Casi Siempre
23	30,00	9,00	5,00	5,00	5,00	24,00	5,00	7,00	7,00	5,00	Casi Nunca	A Veces	Nunca	Nunca	Nunca	Casi Nunca	Nunca	Casi Nunca	Casi Nunca	Nunca
24	35,00	10,00	6,00	6,00	6,00	37,00	7,00	9,00	10,00	11,00	A Veces	A Veces	Casi Nunca	Casi Nunca	Casi Nunca	A Veces	Casi Nunca	A Veces	A Veces	A Veces
25	33,00	9,00	6,00	8,00	6,00	34,00	8,00	9,00	9,00	8,00	Casi Nunca	A Veces	Casi Nunca	Casi Nunca	Casi Nunca	Casi Nunca	Casi Nunca	A Veces	A Veces	Casi Nunca

Vista de datos | Vista de variables